facebook

January 31, 2012

VIA ELECTRONIC DELIVERY

Mr. Donald S. Clark
Office of the Secretary
Federal Trade Commission
Room H-113 (Annex E)
600 Pennsylvania Avenue NW
Washington, DC 20580

RE: *Face Facts: A Forum on Facial Recognition Technology* -- Project No. P115406

Dear Secretary Clark:

Facebook appreciates the opportunity to comment on the issues raised at the Federal Trade Commission's workshop, *Face Facts: A Forum on Facial Recognition Technology*. We applaud the Commission's effort to promote important stakeholder discussions regarding the privacy implications of facial recognition technologies and are grateful to have had the opportunity to participate in the workshop.

Face Facts successfully brought together government, public interest organizations, academics, and the private sector to explore how facial recognition technologies are employed and how to inform and empower consumers so that they can make choices about the use of their information in connection with these technologies. Although the panels featured lively debate, and many different perspectives were represented, two common themes emerged from the day's discussions:

- First, facial recognition technology can benefit consumers if it is employed responsibly and in a privacy-protective manner. As we describe in these comments, Facebook is committed to using this technology in a way that enhances people's online experience while giving them control over their information.

- Second, the privacy and security implications of facial recognition vary greatly depending on the context in which the technology is employed. Because protecting privacy is ultimately about honoring consumers' expectations with respect to their personal information—which may vary significantly depending on the context in which their information is provided and used—many panelists explained that any effort to understand the implications of facial recognition should start with the various uses of the technology.

Facebook encourages the Commission to consider these areas of consensus and to protect innovation by examining the issues raised by facial recognition as it does other issues that may impact consumer privacy: with a "flexible and evolving approach . . . designed to keep pace with a dynamic

marketplace."[1] As the Commission and the Department of Commerce stressed in their draft reports on updating the nation's consumer privacy framework, any approach to protecting privacy must be implemented in a way that empowers consumers to make informed choices about their personal information while ensuring that the innovation that drives the nation's digital economy is not unduly hampered.[2]

At Facebook, we view these twin goals as complementary. Developing innovative, social uses of technology while empowering people to make choices about their privacy has been a critical value since our company was founded. As part of our commitment to the principle of privacy by design, our product teams continue to create new tools and resources designed to give people more control over their online experience. These efforts will only gain momentum as we implement the agreement we have entered into with the FTC to formalize and enhance our privacy program.

The development and employment of our "Tag Suggest" tool—which uses a form of facial recognition technology to make it easier for people who want to tag their friends in photos that they upload to Facebook—is a key example of how we build products that are innovative in the ways in which they allow people to exercise control over their information while connecting with friends and family.

We provide a more detailed overview of our Tag Suggest feature below that illustrates how we have integrated privacy by design principles at its very core. As the overview reflects, the privacy implications that arise from facial recognition very much depend on the context in which the technology is used. We conclude with some recommendations as to how the Commission might continue the productive conversation around these technologies that it began at the workshop.

I. Background: Photos and Tagging on Facebook

Importantly, the privacy protections that we have built into Tag Suggest work in tandem with the controls we provide on Facebook to help people organize and share their photos. We therefore provide a brief overview of those tools before moving onto a discussion of Tag Suggest.

One of the most popular uses of Facebook is to manage and share photos, in part because our photo management tools build upon the things people always could do with their photos—like organizing photos in albums and adding captions—by making those photos social. On Facebook, people can add a special link, called a "tag," to a photo that adds the person to the audience of people that can see the tagged content and suggests they add it to their timeline.[3] In other words, tagging is a special way or linking or adding a name that makes sure the person tagged is aware of the connection and, as

---

[1] Fed. Trade Comm'n Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* 3 (Dec. 1, 2010) [hereinafter FTC Preliminary Staff Report].

[2] *See* FTC Preliminary Staff Report at 3; Internet Policy Task Force, Dep't of Commerce, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* iii (Dec. 16, 2010) [hereinafter Commerce Green Paper] (any privacy framework must "allow innovation to flourish while building trust and protecting a broad array of other rights and interests").

[3] As noted above, a photo tag is a special kind of link on Facebook that suggests the tagged person add the post to their timeline and, unlike a link, can be removed in some cases. We include information about other kinds of links and how they work in our Help Center, at https://www.facebook.com/help/links/.

described below, can exercise control. The availability of tagging—and the ability to interact around photos—has helped make photo sharing one of our most popular features.

We are proud of the innovative ways in which we built privacy into the product. Indeed, we have designed our photo and tagging tools with our goal of empowering people to exercise control over the sharing of their information specifically in mind. For example, our service incorporates:

- Inline privacy controls. Whenever people share content (including photos) on Facebook, our inline audience selector controls enable them to determine the audience with whom the content will be shared. Importantly, these controls are available "at the time and in [a] context in which the [person] is making a decision about his or her data"[4]: they are quickly and easily accessible where and when the content is shared. People can make choices about photo privacy on an album-by-album or even a photo-by-photo basis.

- Tag notifications and tag removal. Facebook automatically notifies people when they are tagged in a photo. This notification creates an opportunity for them to connect and discuss shared experiences, but it also lets them stay informed about how photos of them are being shared on Facebook. If a person chooses to do so, she can "untag" a photo in which she appears, thus unlinking it from her account. This aspect of our photo tagging feature therefore empowers people to learn about the sharing of photos containing their image and to exercise control over whether those photos are associated with their profiles.

- Tag review. Through our Tag Review feature, a person using Facebook has the chance to review and approve or disapprove any photo of her *before* it appears in her timeline. And if a person is tagged by someone who is not her friend on Facebook, she will be given the opportunity to review the tag regardless of whether she has previously enabled Tag Review. Again, this feature empowers people to control the sharing of information in a manner that would not be possible in the absence of tagging.

- Other privacy controls. Facebook's privacy settings also allow people to block others who tag them in photos, which not only removes the tag but also prevents the blocked person from tagging or even contacting the tagged person again. Also, every photo on Facebook contains a "Report This Photo" link, which informs Facebook of abusive photos so that, if necessary, we can take appropriate action.

II. Facebook's Tag Suggest Tool Enhances People's Online Experiences While Protecting Their Privacy.

By helping people organize and share their photos in a way that protects their privacy, tagging has become the single most popular feature on Facebook. But, as with all our services, we constantly strive to make this feature more responsive to the needs of the people who use Facebook. After we introduced tagging, many people told us that it was a useful tool but that manually entering tags for each person in every photo required a great amount of time and effort. As people uploaded more and more photos to Facebook, this issue became more significant.

---

[4] FTC Preliminary Staff Report at 57-58.

In response to this feedback, we developed our Tag Suggest feature, which uses a technology similar to that used for years by desktop photo editing tools and by companies such as Google and Apple. The technology works by taking some of the tagged photos that are associated with a particular person's account; comparing what the photos have in common; and storing a summary of the data derived from this comparison. When a person uploads a new photo, we compare that photo to the summary information of the person and the friends with which she communicates most frequently and suggest a tag, which the person uploading the photo is free to accept or reject.

A. Tag Suggest Was Designed With Privacy At The Forefront.

Throughout the process of designing and deploying Tag Suggest, we considered how to implement the technology in a manner that would enhance people's experience on Facebook without diminishing their ability to control their information. As several panelists explained during the *Face Facts* workshop, facial recognition technology can be used for many different purposes, including for targeted advertising and by law enforcement. Some privacy advocates also have expressed concern that the technology may be used by governments, for example, to identify political dissidents or protesters.[5] Each of these uses presents its own unique privacy considerations.

We built Tag Suggest in a way that specifically addresses the range of privacy concerns that has been expressed about facial recognition technology. First and foremost, Facebook's technology does not depend on surreptitiously collected facial recognition information. Rather than capture facial recognition data without people's knowledge, the only information we use to power Tag Suggest is derived from data people voluntarily have posted on Facebook, and we affirmatively notify people if someone else tags them. Also, we do not use facial recognition technology for the purposes that raised the most concern at the workshop, such as to conduct (or allow others to conduct) surveillance of any kind, let alone surveillance of political activities or to condition pricing or benefits on the basis of conclusions drawn about a person from his or her facial recognition data.

Instead, we only use Tag Suggest to improve our tagging feature by taking data people have given us (namely, photos and the tags people have applied to them), analyzing that data, and using it to make predictions when a person uploads a photo about whether they or one of their most frequently-contacted friends may be in that photo. As the Department of Commerce recognized in its December 2010 "green paper" on revamping the nation's privacy framework, the ability to derive data from other information provided by people often leads to significant innovation.[6] For example, deriving useful data based on an analysis of information that website users voluntarily provide is what enables popular technologies such as recommendation engines like those used by Amazon and Netflix. Those technologies use people's purchase and rating information in order to make predictions about products

---

[5] *See, e.g.*, Paisley Dodds & Raphael G. Satter, *London Riots 2011: Facial Recognition Technology Considered for Olympic Games Used to Identify Rioters*, Huffington Post, Aug. 11, 2011, http://www.huffingtonpost.com/2011/08/11/london-riots-2011-facial-recognition-technology_n_924282.html; Lesley Ciarula Taylor, *How facial-recognition software could track down G20 suspects*, Toronto Star, July 15, 2010, http://www.thestar.com/news/gta/article/836304--how-facial-recognition-software-could-track-down-g20-suspects; Naomi Klein, *China's All-Seeing Eye: A Nation Under Surveillance*, Rolling Stone, May 14, 2008, http://www.rollingstone.com/music/photos/chinas-all-seeing-eye-a-nation-under-surveillance-20080522.

[6] Commerce Green Paper at 38-39.

or services they (and others with similar interests) might enjoy. These applications are useful specifically because of their ability to use conclusions derived from data that people intentionally give them. And, because they are not collecting any new data surreptitiously, the privacy concerns that they raise are limited.

The FTC's staff reached a similar conclusion in its 2010 preliminary staff report, which suggested that a first-party website's use of people's data to make recommendations and improve its service may raise fewer privacy concerns than other data practices and thus may not require choice.[7] This reasoning applies with equal force in the facial recognition context. On the one hand, services like Tag Suggest use derived data in a manner similar to recommendation engines. That is, for example, Tag Suggest simply looks at the photos and tags that people add to Facebook and makes predictions about who might be in a particular photo. The people who provide this data have established relationships with Facebook and use our service because they want to share information about themselves with friends and family in a safe and controlled way. On the other hand are those implementations of facial recognition that rely on the direct, surreptitious collection of data from people with whom the collector has no preexisting relationship. The privacy issues raised by these implementations are fundamentally different from those that arise from the use of technologies like Tag Suggest.

Of course, any analysis and use of people's data, however innovative, must take place with due regard for privacy. But when the privacy interests in a particular transaction are limited—as they are in the examples involving derived data discussed above—a more restrained approach on the part of government is appropriate. By contrast, the uses of information collected by a faceless company without a person's knowledge may raise more significant privacy issues and require greater strictures. In the end, what is important is that regulators take a flexible approach in their assessment of the privacy implications of a particular data transaction.

B. Facebook Provides Meaningful Control Over The Use of Information in Tag Suggest.

In addition to the difference in the way Facebook *collects* information to enable its Tag Suggest feature, there is also a stark difference between the ways Facebook *uses* this technology as compared with other uses. In contrast to uses of facial recognition technology that allow unilateral identification of people without giving those people the ability to control the experience, we have designed Tag Suggest so that it only helps recognize people who have already agreed to connect with one another.

In addition, the comparison that takes place when someone uploads a photo to Facebook is not to a database of every photo on Facebook, or even selected photos of every Facebook user. Instead, Tag Suggest works with data that has been derived from photos of the person's most frequently-contacted friends on Facebook. Facebook's technology does not allow a person to upload a photo for the purpose of finding "matches" from among a large group of unknown individuals, as do some of the other implementations about which panelists expressed concern at the workshop.

The privacy implications of these design choices are significant. Facebook's technology uses data that is not surreptitiously collected from a suggested person, but rather is derived from "tags" that the person has added to photos directly or of which she has been notified and given the opportunity to remove. Because people can control the photos in which they are tagged, they can control what data

[7] Preliminary Staff Report at 53-55.

Tag Suggest may use to identify them. As Tag Suggest, like the Facebook service more generally, continues to evolve, we will continue to build privacy protections into the product. As a part of that effort, and consistent with our recent agreement with the FTC, we will make changes to our product only after a comprehensive review that is designed to identify any privacy risks associated with a change and to implement appropriate controls to address any risks that we identify.

We also give people the ability to disable Tag Suggest altogether by changing their privacy settings. Moreover, as the Irish Data Protection Commissioner's Office concluded following its recent audit, when someone chooses to disable Tag Suggest, we delete the summary data about him or her that powers the tool.[8] These controls provide meaningful choices that are appropriate to the context in which the technology is used.

Some have suggested that facial recognition technology should always be used on an opt-in basis and have urged Facebook to require people to opt in expressly before data derived from photos in which they are tagged may be used in Tag Suggest. These suggestions, however well-meaning, fall into the trap of assuming that one kind of consent is appropriate for all circumstances. As the FTC staff acknowledged in its recent privacy report, that perspective fails to take into account the importance of context and can actually result in controls that are *less*, rather than more, privacy protective.[9]

When we build privacy controls at Facebook, we recognize that one size does not fit all, and that requiring people to opt in individually to every aspect of Facebook would not only fail to adequately protect privacy but quickly make the Facebook service difficult to use. As an example, Facebook lets people choose an audience—for example, "friends only"—for individual status updates. If a person posted a status update as "friends only" and then explicitly opted into each of her Facebook friendships, requiring the person then to approve each friend to be able to see that update on her Timeline, and again in each friend's News Feed, would be duplicative and unnecessary. We do not believe that people expect to be required to opt in multiple times to the various ways they can communicate with friends on Facebook, particularly when Facebook offers granular controls that help them control their experience. In fact, people might simply have tired of the demand that they opt in repeatedly and, because of the burden, chosen not to do so, preventing their status updates from having their intended effect.

In contrast, there are circumstances in which opt-in consent is the most effective way to give people control on Facebook. For instance, if a person tries to use a new third-party application on Facebook that will need information from her Facebook account in order to work, we identify the application, explain what information is required, and give the person the choice whether to allow the application to have the requested access. We also let the person change her mind later, and when she does we require the application to delete any information that it previously obtained about her. In contrast to the communications described above, which are within the context of an existing opt-in relationship, the use of a new third-party application is a distinct context in which information is shared, and we believe that our approach is the most efficient way to give people control over that sharing.

---

[8] Facebook Ireland, Ltd., Report of Audit of Irish Data Protection Commissioner, p. 103 (available at http://dataprotection.ie/viewdoc.asp?DocID=1182&m=f).

[9] FTC Preliminary Staff Report at 60 ("[A] clear, simple, and prominent opt-out mechanism may be more privacy protective than a confusing, opaque opt-in.").

Regardless of the specific feature at issue, we recognize that the decision how best to give people control over their experience is a very product-specific one. It involves a range of considerations, including the context in which the person is using the feature, the expectations that Facebook users have about how the feature will work, and the mechanism that empowers people to make choices without interfering with those expectations.

Facebook's Tag Suggest feature, unlike other facial recognition products that create greater privacy concerns, is based specifically on individual control. It makes suggestions based on the networks that people have formed expressly on Facebook, rather than seeking to identify unknown people. And it further empowers people to control the experience, even within those expressly created networks, by notifying them when they are tagged and giving them a range of choices about how information derived from that tag will be used. In light of the way we have chosen to implement the technology, we do not believe that people want or need to satisfy an additional hurdle before using our Tag Suggest feature.

C. Facebook Provides Strong Safeguards For the Personal Data Used by Tag Suggest.

In addition to providing appropriate privacy controls, we believe that it is important to implement appropriate security and procedural safeguards for the personal information that we store. To that end, we encrypt the summary data that we derive from tagged photos and limit the ability of people within Facebook to access this information.

In addition, our internal policies restrict our disclosure of this information to government agencies. This limitation is particularly important in this context, because, as comments during the *Face Facts* workshop demonstrated, many people's apprehension about the commercial use of facial recognition stems from the perception that information gathered by private entities could be shared with government actors. As we describe in our Data Use Policy, we sometimes provide information from our databases to the government where required by law or where necessary to protect public safety. We have a dedicated team of certified privacy professionals that scrutinize each disclosure request that we receive to ensure that the request complies with strict requirements, such as specificity about the person who is the target of the request and the information that is sought. Facebook is committed to complying with the limitations of law and our Data Use Policy when responding to government or law enforcement agency requests for information.

Ultimately, though, we do not believe our Tag Suggest data would be useful in a law enforcement context because law enforcement agencies already have their own facial recognition software that is better suited to law enforcement purposes than our Tag Suggest technology. To the extent that any information in Facebook's possession would be of use to law enforcement, it would be the photos that people upload themselves, not the limited data that we derive from those photos to make it easier for people who want to tag through our Tag Suggest feature.[10]

* * *

[10] Of course, the best way to address concerns about how law enforcement agencies might use the photos stored on Facebook or other photo sharing websites is not to regulate people's ability to store or share photos online. Instead, guidelines—such as Facebook's *Facebook and Law Enforcement* guide, available at http://www.facebook.com/safety/groups/law/—can be established to help law enforcement agencies properly limit the way that they use people's data.

Tag Suggest exemplifies Facebook's commitment to implementing privacy by design in an innovative way. Moreover, as demonstrated above, Tag Suggest's privacy-protective features serve as useful points of contrast for implementations of facial recognition technologies in other contexts. These key distinctions we have noted highlight a larger, more fundamental point that should inform the Commission's thinking about the implications of these technologies: facial recognition is used for a variety of purposes and consumers have widely varying abilities to control that use.

For this reason, as we move the discussion forward, it is important not to conceptualize facial recognition as a monolithic concept with uniform implications for privacy, but rather as a general category into which many activities—with varying privacy implications—might fall. Sensitivity to the different implementations of facial recognition can help us assess the privacy implications of these technologies in a more precise way. As we discuss in the next section, it is important that any understanding of the implications of facial recognition take into account the variety of uses of the technology.

III. An Understanding of the Privacy Implications of Facial Recognition Must Account for the Variety of Contexts in Which It May Be Implemented.

Like many of the other technologies that the Commission addressed in its December 2010 preliminary staff report, the policy implications of facial recognition technology depend greatly on the contexts in which the technology is implemented. As illustrated above, the privacy issues that arise from using facial recognition to surreptitiously identify a person in the first instance are very different from the issues involved in using the technology as a tool to organize photos of friends. And these different issues mean that different privacy protections may be appropriate depending on the context in which facial recognition is used. Considering the context in which information is collected and used in connection with facial recognition technologies is crucial because context necessarily shapes consumers' privacy expectations. This, of course, is not only true for the collection and use of information in connection with facial recognition technologies but for data practices more generally.

The FTC has long understood the importance of context in evaluating whether a company's practices honor consumers' privacy expectations. Because of this, the Commission has generally refrained from advocating specific legislation or regulation of particular technologies that may have implications for consumer privacy. Instead, the FTC typically has urged businesses to conform their conduct to broad principles that may be implemented in different ways depending on the needs and expectations of consumers in a particular context.

The FTC's earliest efforts to ensure that consumer privacy was protected online involved its encouragement of businesses to adhere to "fair information practice principles," which embodied basic concepts of transparency, consumer empowerment and industry accountability. This approach emphasized four principles—notice, choice, access, and security—and recommended that these principles be implemented by businesses across the online space. Importantly, these principles were technology-neutral and designed to be flexible enough for businesses to incorporate them in a wide variety of contexts.

The preliminary staff report proposed to update these principles for the digital economy of the twenty-first century. Although the report is organized around a new group of key concepts, the Commission's overall approach to consumer privacy is still based on the notion that a framework of flexible, general principles is the best way to ensure companies' adherence to baseline privacy

protections in a rapidly changing marketplace. The Department of Commerce has advocated a similar methodology, stressing that broad principles should guide efforts to implement privacy protections across different industries.

Facebook supports a principles-based approach to protecting consumer privacy. Encouraging baseline principles is the best way to ensure that consumer privacy is protected across industries and technologies while also accounting for the fact that specific protections will depend on the contexts in which a consumer's information is collected or used. A principles-based approach, rather than specific legislation or regulation, also stands a better chance of remaining strong as technology—and consumer expectations—continue to evolve. Efforts to protect privacy in connection with a specific technology or practice risk being outmoded by unanticipated technological developments.

The principles-based approach that the Commission has consistently advocated should inform its thinking about facial recognition technologies. An approach that subjects information collected or used by facial recognition technologies to specific treatment risks being, at once, both too broad and too narrow. Such an approach risks being too broad by treating all facial recognition technologies similarly when, in fact, different implementations give rise to widely differing privacy implications. This approach also risks being too narrow because it may not be flexible enough to account for the inevitable evolutions of these technologies over time, and consumers' changing privacy expectations with respect to them.

Apart from being ineffective, a targeted approach to facial recognition is likely unnecessary given that the framework the Commission currently is developing will likely be sufficient to assess whether a particular implementation of facial recognition is consistent with consumers' privacy expectations. For example, in evaluating whether a particular implementation of facial recognition is sufficiently privacy-protective, the Commission could use the lens of its core principles of privacy by design, choice and transparency:

- Privacy by design. In assessing a particular use of facial recognition, the Commission could consider whether it incorporates key substantive protections. For example, was the technology designed to identify people that the user of the technology otherwise could not identify, or as tool for managing photos? Was the technology designed to surreptitiously capture consumers' information or to use data that consumers have provided voluntarily?

- Choice. The Commission also could consider a person's ability to control the use of his or data in a particular implementation. Can a person learn what data has been collected? Can the person control how it used? Can the person delete the information altogether?

- Transparency. Does the entity that uses facial recognition technology provide consumers with clear notice of its practices? Or is the information collected about the person secret and used only in ways of which the person is unaware and cannot control? Does the entity offer channels for consumer feedback and adapt its services in response to such feedback?

In other words, we suggest that in evaluating the policy implications of a facial recognition implementation, the Commission consider the use to which the implementation is put and then assess whether core principles of privacy protection are honored. As these considerations illustrate, the aspect of a facial recognition implementation that informs its privacy implications is not the simple fact that it involves facial recognition, but rather the way in which the technology is used. In this regard, we believe

that the approach to privacy in the facial recognition context should be principles-based and technology-neutral so that individuals receive the same protections for their information regardless of what kind of software is used to generate or process that information.

In sum, Facebook believes that facial recognition technologies can benefit consumers if they are implemented responsibly, and we are strongly committed to doing so. We appreciate the opportunity to engage with the Commission and other stakeholders on this important issue, and will look forward to continuing the conversation in the future.

Respectfully submitted,

Erin M. Egan
Chief Privacy Officer, Policy
Facebook