The Privacy Surgeon

26th November 2013

Complaint lodged with the Data Protection Authorities of Norway, Sweden, Czech Republic, Denmark, France, Spain, Italy, Slovenia, Austria, Belgium, Germany (Federal and Berlin), Lithuania, Netherlands and Poland.

Dear Commissioner,

Complaint: Change of Google's Terms of Service - "Shared Endorsements"

I am writing with regard to recent changes to Google's Terms of Service and to lodge a complaint with you over consequent data protection violations. My complaint focuses primarily on the new "Shared Endorsements" policy, but is also relevant to a number of other recent policy changes made by the company.

On the basis of my initial assessment it appears that the changes will substantially violate Data Protection law, and I request that your office institutes an investigation. I also ask that you intervene on behalf of European nationals to seek the immediate suspension of the changes pending the outcome of your investigation.

Background to the Shared Endorsement policy

On November 11th 2013 Google activated a new policy[1] that exploits the images, personal data and identities of its users to construe personal endorsements published alongside the company's advertised products across the Internet. Personal and identifiable data is used to enable these endorsements.

The new policy allows the company to include adult users' names, photos and comments in ads based on ratings, reviews and posts they have made on Google Plus and other Google services like YouTube. Google is now able to show automated Shared Endorsements on the more than two million sites in Google's display advertising network.

This means if a user follows a car manufacturer on Google Plus or gives a music artist four stars on the Google Play music service, for example, that user's name, photo and endorsement could show up in ads for that car or artist.

[1] https://plus.google.com/settings/endorsements

This initiative should be seen in the broader context of other changes recently made to Google's Terms of Service that require users to log in or to create a Google+ account before being permitted to leave comments on YouTube. Not only are users now required to disclose their identity in order to interact on YouTube, but they are, by default, liable to have those comments and views construed as product endorsements in a generally visible publicly and identifiable format.

Users may opt-out of the Shared Endorsement scheme. I will focus on deficiencies in the opt-out later in this complaint.

The endorsements are not limited merely to the outcome of Google searches. Google ads are a vast global business and a person's face could show up on any of the two million sites that are part of the Google ad network.

The technology is centred on a user's Google+ identity, and it could be difficult for users to avoid Google+ within the new system. The social network and user identity hub has been steadily grafted onto all of the company's popular services. Even if users believe they do not have a Google+ profile, there's a good chance that one has been automatically created if they use Google's other services.

Indeed all new users looking to create an account on YouTube, Gmail or any other Google product are now required[2] to sign up for both Google+ and a Gmail account. Previously, an existing email address would allow users to set up an official Google Account. Now a name, Gmail username, Google+ account and gender are required.[3] Thus a seamless data freeway between services is created that maximises the use of personal information.

In this way Google has triangulated the exploitation of user data by requiring users to create accounts that are content-scanned, by merging their data throughout the Google ecosystem and then by linking personal preferences, interactions, associations and views to its advertising network. This can be viewed as a "Perfect Storm" for online privacy.

Although relating to a somewhat different legal context it is useful to note comments made by US Senator Edward Markey, who recently sent a letter to the Federal Trade Commission asking if Google's Shared Endorsements violates the company's 2011 privacy settlement with the FTC over its now-defunct Buzz service.

> *"This shift in Google's policy raises a number of important questions about whether Google is altering its privacy policy in a manner inconsistent with its consent agreement with the Commission and, if the changes go into*

[2] http://googlesystem.blogspot.nl/2012/01/new-google-accounts-require-gmail-and.html
[3] http://marketingland.com/google-now-forcing-all-new-users-to-create-google-enabled-accounts-3912

> *effect, the degree to which users' identities, words, and opinions could be shared across the Web."* [4]

In response to critics and their concerns over privacy implications of the new changes, Google commented: "The privacy and security of our users is one of our top priorities. We believe our Terms of Service updates are a positive step forward in clarifying important privacy and security details for our users, and are in full compliance with the law." [5]

Background to Google's regulatory compliance in Europe

Google has a long history of privacy infringements in Europe. This section identifies some issues this history has created in the European community and explains why Google is likely to continue infringing European laws unless remedial action is taken by regulators. It also explains how Google's latest update to its Terms of Service is yet another example of how Google cuts corners at the expense of user privacy and control.

Google represents one of the most significant threats posed by the private sector to the online privacy of European citizens. Over the last half-decade, Google has been the subject of more investigations by European Member State privacy regulators – and has been fined and otherwise sanctioned more times and in more Member States – than any other multinational company. Google now is the subject of yet another privacy enforcement action, involving DPA's of six separate Member States.[6]

Despite regulatory actions, however, Google's behaviour to date appears to remain unchanged. As reflected by Google's recently-revised Terms of Service, Google continues to make new uses of European citizens' personal data in ways that fail to respect European law and consumers' rights.

The reason for this systemic violation appears to be Google's core business, which is advertising. Ad sales made up 95% of Google's revenues in 2012. Google services are free of charge to users, but users effectively pay for them with their personal data, which Google then leverages to generate advertising revenue. Google's appeal to advertisers is that it has accumulated a massive trove of user data and can use that data to profile how users act and behave – enabling advertisers to target advertising more precisely and effectively. Google's revenue and growth therefore is linked directly to – and indeed is reliant on – Google's ability to collect and share data about users.

---

[4] http://news.cnet.com/8301-1023_3-57607247-93/senator-to-ftc-does-google-ad-change-break-privacy-deal/

[5] http://online.wsj.com/news/articles/SB10001424052702304066404579129850887794072

[6] http://www.cnil.fr/english/news-and-events/news/article/google-privacy-policy-six-european-data-protection-authorities-to-launch-coordinated-and-simultaneo/

In other words, Google cannot afford to stop collecting data about its users. That is why Google's actions continuously come into conflict with European (and U.S.) privacy laws. Unlike other types of regulation, privacy laws are not just a matter for Google's administrators to follow. By limiting how much data Google can collect, how long Google can store data, and the purposes for which Google can use the data, European data protection laws pose a threat to Google's business model. Put differently, Google's business model is explicitly at odds with European principles of privacy protection. The result is a string of infringements that stretch back over the last half-decade, such as the Street View WiFi interception,[7] hacking of the Safari privacy preferences,[8] Google Analytics, Google Apps[9] and the move to a Single Privacy Policy.

Google's move to a single policy immediately raised concerns for European privacy regulators, who repeatedly asked Google to delay launching the policy which they believed[10] breached European data protection laws. Google refused, and launched its policy despite the requests. In October 2012, after Google failed to fully answer the CNIL's questions, the CNIL issued a set of recommendations for Google to implement to correct its conduct. Google has so far refused to implement any of the CNIL's recommendations.

On 11 October 2013, despite pending enforcement actions by European regulators as a result of Google's move to a single privacy policy, Google announced that it was changing its online Terms of Service. The primary change, as explained by Google, was to "[clarify] how your Profile name and photo might appear in Google products (including in reviews, advertising, and other commercial contexts)." In other words, Google's new Terms of Service will allow Google to use the Profile names and photos of its users to expand the types of advertising it can target at its users. This will help Google grow its revenue by offering new types of "friend-based" advertising – but the change also demonstrates how Google continues to trade the privacy of its users for its own commercial gain. In effect, Google has moved beyond monetising user data and is now monetising users themselves.

The new changes go against the specific October 2012 recommendations that European privacy regulators made to Google. Google proposes to use the fully combined user profiles that it compiled under the Privacy Policy – a user's preferences, friends and contact lists, web and search history, and photo – to fuel advertising endorsements. My complaint asserts that Google has gathered these combined user profiles illegally, and must rectify that illegality prior to making

[7] http://www.forbes.com/sites/kashmirhill/2013/09/10/wi-spy-continues-to-haunt-google-federal-court-says-it-may-have-violated-wiretap-act/
[8] http://www.ftc.gov/opa/2012/08/google.shtm
[9] http://www.privacysurgeon.org/blog/incision/swedens-data-protection-authority-bans-google-apps/
[10] http://www.privacysurgeon.org/blog/incision/french-privacy-regulator-finds-google-in-breach-of-national-law-as-spain-and-germany-close-in/

continued use of those profiles for marketing. Google has ignored this guidance, and has instead decided to use this "bad" data in new ways.

Google offered some warning of the change in terms to desktop users, but gave fewer warnings to mobile users, despite the rapid growth of users who access the Internet primarily or even exclusively on a daily basis via smart mobile devices.

Despite Google's assurance that "the only people who see [ads you have endorsed] are the people that you've chosen to share that content with," endorsements through some services, like Google Plus Local, are public, so a user's endorsement in some scenarios, likely to their surprise, could be used in ads seen across the Internet.

European regulators also recommended to Google that it provide its users with more effective and granular user controls over the company's use of user profiles. But Google only offers users a choice to opt-out of this type of "advertisement endorsement" by un-checking a pre-checked "Shared Endorsements" box in their Google account settings. The opt-out is more than Google has offered in the past in other contexts, but it still violates the recommendations of European regulators. For instance, by pre-checking the box, Google has chosen to opt-in users to the new advertising endorsements by default, ensuring that vulnerable and non-privacy savvy users will fail to find or use the opt-out.

Context of the complaint: deception, unlawfulness, unfairness and lack of transparency

It is relevant to note that the approach taken by Google to the privacy implications of the new policy is complex and deceptive. The company has taken minimal steps to meaningfully publicise the change. While the home page does make reference to new terms, clicking on that link merely takes users to a generic page with the headline "We are committed to improving your security, protecting your privacy, and building simple tools to give you choice and control." [11]

Users wanting to understand the nature of the changes would need to then click the "Terms of Service" link on the right of the page, then click the "updates" link on the following page, followed by a "summary of changes" link on a third page. https://www.google.com/intl/en/policies/terms/changes/

However perhaps the most aggressive action by Google can be seen in the form of words used to describe the privacy implications of its new policy.

In its information page on the new terms the company states: "Don't worry, your account's privacy settings are not affected[12]." This is a highly deceptive and

[11] https://www.google.com/intl/en/policies/?fg=1
[12] https://support.google.com/plus/answer/3403513?hl=en

misleading assertion. A user who has created privacy settings for minimum sharing and disclosure would be forgiven for believing that the higher level of privacy protection would be maintained, but this is not the case. The opt-out endorsement control is an entirely separate mechanism that has no relation whatever to the user's pre-existing privacy preferences.

It is logical to presume that the opt-out sharing control is "in itself" a privacy setting. Claiming that the mechanism is not a privacy setting misrepresents the nature of the changes that have been made, inferring that there are few - if any - privacy implications of the new policy. Given the widespread data sharing that endorsements entail, this is clearly not a true depiction of the changed privacy environment.

Over the past few years European Data Protection Authorities and other regulators have stressed the importance of clarity and transparency in the terms and conditions imposed by companies. However media and other observers have noted that Google's terminology is opaque and confusing, leading to unfairness in the relationship with users.

Core issues of the complaint - Specificity and Purpose Limitation

The legal reasoning upon which this complaint is based can be found in Opinion 03/2013 on purpose limitation adopted by the Article 29 Working Party on 2 April 2013.[13]

The legality of recent changes to Google's policies that allow the company to share personal data across all its products and services are currently being investigated by a number of EU data protection authorities. The data protection issues and violations highlighted in my complaint go the heart of many of the aspects under investigation. Indeed the Shared Endorsements policy is made possible only through company-wide amalgamation of personal data.

The dynamics of personal information disclosure are well known to data protection authorities. Users disclose their personal data and their identity on the basis of an awareness of how their data will be used within a particular context. The Google business model - of which Shared Endorsements are a key component - negates this essential element of privacy protection.

Central to this issue is the context for Google+, which the company has always promoted as a platform that encouraged true identities and true image likenesses. Contrast this to the YouTube context, which has traditionally been focused on the nature and content of comments, rather than on identities themselves. The new policy now creates a clash of context in which true identities are associated with

[13] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

personal views.

When users signed up for a Google+ account they were not informed that in order to use other Google services in the future, their data would be used for commercial purposes outside the Google+ environment.

Many users will be unaware of the ramifications of leaving comments and preferences on YouTube and other Google services. Full exposure of identities will be a fact known to some, but not all users.

The central violation of data protection law occurs when data collected and disclosed for one purpose (say, expressing a view within the context of a closed social networking environment), is then published on an open Web platform for advertising and endorsement purposes.

The Article 29 Opinion sets out the foundation position:

> *"Specification of purpose is an essential first step in applying data protection laws and designing data protection safeguards for any processing operation. Indeed, specification of the purpose is a prerequisite for applying other data quality requirements, including the adequacy, relevance, proportionality and accuracy of the data collected and the requirements regarding the period of data retention. The principle of purpose limitation is designed to establish the boundaries within which personal data collected for a given purpose may be processed and may be put to further use."*

The principle has two components:

> *- the data controller must only collect data for specified, explicit and legitimate purposes,*
>
> and
>
> *- once data are collected, they must not be further processed in a way incompatible with those purposes.*

The Opinion goes on to observe:

> *"Purpose specification is an essential condition to processing personal data and a prerequisite for applying other data quality requirements. Purpose specification and the concept of compatible use contribute to transparency, legal certainty and predictability; they aim to protect the data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing. The limitation should, for example, prevent the*

> *use of individuals' personal data in a way (or for further purposes that they might find unexpected, inappropriate or otherwise objectionable. At the same time, the notion of compatible use also offers some degree of flexibility for data controllers."*

The legal basis for purpose specification is:

> *"Collection for 'specified, explicit and legitimate' purposes Article 6(1)(b) of the Directive requires that personal data should only be collected for 'specified, explicit and legitimate' purposes. Data are collected for certain aims; these aims are the 'raison d'être' of the processing operations.*

Importantly, the Opinion advises that to be explicit, the purpose must be sufficiently unambiguous and clearly expressed. "Comparing the notion of 'explicit purpose' with the notion of 'hidden purpose' may help to understand the scope of this requirement…"

Article 6(1)(b) of the Directive also introduces the notions of 'further processing' and 'incompatible' use, and requires that further processing must not be incompatible with the purposes for which personal data were collected. In particular, Article 6(1)(b) requires that personal data should not be 'further processed in a way incompatible' with those purposes and recital 28 states that the 'purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified'.

Article 6(1)(b) of the Directive further requires that personal data must be collected for 'specified, explicit and legitimate' purposes.

The Opinion elaborates on this requirement:

> *"The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied."*

Given the conditions described above it would be difficult to imagine how Google could reasonably move data from a narrow ecosystem such as YouTube, to an open advertising platform when there is no mention made in its privacy policy of such a shift. Indeed at the time of writing the latest update to the privacy policy was June 24th, more than five months before the Endorsement policy came into effect.

Furthermore, the opt-out mechanism creates a substantial data protection issue. Article 29's Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010, notes "..opt-out mechanisms do not in principle deliver data subjects'

consent." [14]

The Shared Endorsements policy also violates a number of related data protection aspects including reasonable expectation, compatible use, transparency, predictability and user control.

I hope you are able to resolve these matters swiftly to ensure that Internet users continue to enjoy the benefits of online interaction as well as protection of their privacy and personal information.

Yours sincerely,

Simon Davies

[14] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf