



PRIVACY INTERNATIONAL

**2nd Floor, Lancaster House,
33 Islington High Street,
London N1 9LH, UK**

Complaint filed with privacy & data protection regulators of France, Germany, the Netherlands, Greece, Italy, Spain, Czech Republic, Belgium, Denmark, Sweden, Ireland, Portugal, Poland, Austria, Australia and Canada along with the European Commission and the EU Commissioners internal Article 29 Data Protection Working Group (amended according to the relevant national legal environment)

Complaint: Google Inc – Gmail email service.

19th April 2004

I am writing with regard to a new Webmail service that is being established at an international level by Google Inc, a US based company that operates the world's most popular Internet search engine.

You may be aware that Google announced on April 1st this year that it will offer an email service which will provide each customer with one gigabyte of storage space. That is, around 500,000 pages of email per user. The service is being promoted as a means of creating a centralised and permanent archive of all email. Gmail says "Google believes people should be able to hold onto their mail forever." (1) While this may not currently be possible even at the one gigabyte level, the availability of the Gmail service will entice many users to maintain a single account, rather than having several, as many currently do.

However, the Gmail service will electronically scan the subject headers and contents of all these private emails to generate targeted advertisements relevant to the email content.

The Gmail service has already prompted substantial criticism from privacy and consumer groups both in the US and in Europe. (2) It has also generated a considerable amount of media controversy (3). Privacy International and many of its members across Europe are concerned that this service, currently in its Beta testing stage, violates a number of elements of Data Protection law.

This complaint is made under subject rights set out in Data Protection legislation, and also within the terms of Article 20 of Directive 95/46/EC of the European Parliament and of the Council (the Data Protection Directive) that stipulates:

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof. (4)

The market for webmail services is substantial. The top three webmail companies have well in excess of 250 million unique users worldwide with a probable total market of a hundred million users in Europe. Google's supremacy in the search market will ensure that it stands a strong chance of challenging the major players.

While the majority of Gmail users are likely to be individuals, there will be a substantial number of small businesses and other enterprises using the system – in time possibly numbering in the millions within Europe. These organisations are required to fulfil a range of conditions under data protection law. It is our contention that the Gmail service will not allow these requirements to be fulfilled.

The precedent set by Google is likely to lead to a global trend to greater US based centralisation and storage of personal emails and a more comprehensive linkage between content and advertising. Google's competitors have already moved to increase their storage capacity.(5) This increased storage and functionality will fundamentally change the privacy expectation for electronic communication and will create additional security and data protection threats.

You may be aware that data storage devices have been increasing in capacity even faster than computing power. The capacity of underlying recording media has been roughly doubling in size by area every 12 months¹. This should continue over the next few years, leading to an approximate 30-fold increase in capacity over five years. The price of storage has now dropped to the point where it has become at most a secondary cost-factor in large systems. This is why the Gmail offering is likely to eventually extend throughout the entire email market.

Such a large increase in storage space not only allows the creation of greater reserves of data, but it will also facilitate the retention of more precise and finely grained levels of data (e.g. higher resolution and frame rate video). Increased storage capacity will also make possible the retention of entirely new types of data.(6)

Hence, we believe it is crucial at this stage to assess this type of service with a view to ensuring that all necessary protections and safeguards required by the EU Data Protection Directive and national laws have been implemented. While we understand that the Gmail contract may be freely entered into by customers, and that Google has provided a degree of openness about its intentions, the conditions must be in place to ensure that privacy rights are protected.

¹ Andreas Moser, Kohji Takano, D. T. Margulies, M. Albrecht, Y. Sonobe, Y. Ikeda, S. Sun and E. E. Fullerton. Magnetic Recording: Advancing into the Future, *Journal of Physics D*, vol. 35(19):PR157-67, October 2002. Available from stacks.iop.org/JPhysD/35/R157

You may be aware that in its Working document “Privacy on the Internet”, the Article 29 Data Protection Working Party identified a clear need to specify the concrete application of the rule on applicable law of the general data protection directive (Article 4 paragraph 1 (c)), in particular to on-line processing of personal data by a controller established outside the Community. This complaint is pursuant to this concern.

I am writing to set out our concerns and to ask that you investigate the Gmail service with regard to compliance with Data Protection.

If you determine that the planned service violates Data Protection law I would request that you notify Google that the service should be modified, and that regulatory action may be taken to prevent the service being offered. If the outcome of this process is not satisfactory I would request that an order may be made to prohibit the export of personal data to Google.

The Service

Google will offer users one gigabyte of email space. This is an unprecedented level of storage. Costs of the service will be recovered through the generation of targeted advertisements that will appear – as they currently do with Google searches – in the right hand margin of the page.(7)

The service employs technology that automatically scans the content of emails and then uses a keyword-matching programme that sifts the placements of Gmail advertisers. Relevant advertisements will appear not just on the computers of Gmail account holders, but also on the computers of other Gmail customers they communicate with.

The practicalities of the Gmail search & target system have been described as follows:

A colleague who also got an early Gmail account received a link to *Newsday*, apparently because an e-mail in his inbox had references to *The New York Times* and National Public Radio. When he mentioned this to me in yet another Gmail message, I received links to the *New York Post* online edition and to a site called TheFirstTwins.com. As we continued the dialogue, I got sponsored links to the *Times*, plus newspapers from the United Kingdom. (8)

The service will utilise a unique combination of conventional technologies and techniques already being employed both by Google and by other search and email services.

It should be remembered that a large amount of associated and inferential information is connected to use of such services. Google announced last week that it is now selling geographically targeted ads for its search engine ad placements. So, if a user lives in London, then London advertisers can purchase ads just for that geographic area. This is being done through geographic analysis based upon the logged IP address of the user. The point here is that Google is targeting ads closely. Gmail will greatly help it in doing this via the cookie and IP correlation.

Additionally, Google has a history of logging consumer information via its search site. It logs users' search terms by IP address and unique cookies. One can see this easily (at least the IP logging and keyword logging) via Google Zeitgeist, a page where Google lists the most popular terms that individuals across the world have used for the past years. This data is aggregate. But the material they sell to advertisers is quite sophisticated. Gmail would be no different, except that the data could be tied to an individual for the first time on a mass scale.

The issues we raise in this complaint are not all unique to Gmail. However, it is the scale and functionality of the Gmail service that poses a heightened level of threat to the rights of individuals and to the security and privacy of communications. At a more general level, the service – like others of its type operating in the US where there is an absence of equivalent legal protections – appears to violate EU data protection law.

The Google Privacy Policy & Terms of Service

The Google Privacy Policy (9) and Terms of Use (10) provide an insight into the environment in which Gmail will operate. These documents give rise to a range of concerns about the ability of the Gmail service to comply with European data protection provisions. While the privacy policy appears to provide many of the conditions and notifications that we would expect from such a service, the Terms of Use leave much to be desired.

While a number of the issues below are outside the jurisdiction of most data protection regulators, we feel they are important indicators to establish the circumstances surrounding the operation and use of the Gmail service.

Stability of the contract

The Google contract is unstable. Customers should be confident that the safeguards and protections contained in a contract would be maintained. However, the Gmail Terms of Use state:

Google may, in its sole discretion, modify or revise these terms and conditions and policies at any time, and you agree to be bound by such modifications or revisions. If you do not accept and abide by this Agreement, you may not use the Gmail service.

This condition gives rise to some concern. A service that will create a central reserve of a user's emails over many years must be afforded long term protection. It is a highly sensitive, valuable and vulnerable resource, and must be subject to a guarantee of long-term safeguards.

It is usual for companies offering “free” services to feel they can impose such conditions. However, the Terms of Use represent an agreement of mutual benefit to both the company and to the user. It is thus a contract involving binding conditions. Under the traditional law of contract there should be a minimum of disruption to these terms. Certainly, any change should be conditional upon a degree of foreseeability. No such conditions exist in the contractual environment set out by Google.

The following conditions also involves a serious degree of uncertainty and unreliability:

Google also reserves the right to modify, suspend or discontinue the Service with or without notice at any time and without any liability to you.

And also:

Google reserves the right to refuse service to anyone at any time without notice for any reason.

While we accept that similar conditions have been instituted by other communications providers we feel the unequivocal nature of these clauses require modification. It is certainly true that communications providers in Europe have imposed similar conditions, but the rights of consumers can be enforced through local law. Such is not the case when dealing with a non-EU provider. This is why the Gmail contract must be more detailed and rigorous than would be the case if it were based in the EU. The contractual solutions pursued by the EU with regard to offshore processing reflect this imperative.

Security of data

Under Section VIII article 17 of the EU Data Protection Directive a data controller must take full responsibility and accept liability for the security of personal information. This applies equally when the data is processed outside the EU. However, the Gmail Terms of Use state:

Google disclaims all responsibility and liability for the availability, timeliness, security or reliability of the Service.

This is an unacceptable condition. In our view security must be accorded considerably greater weight within the contract.

Interception and disclosure of content

The privacy of the content of communications must be assured, and any violation of privacy must be subject to due process. However, the Gmail contract states:

Google reserves the right, but shall have no obligation, to investigate your use of the Service in order to determine whether a violation of the Agreement has occurred or to comply with any applicable law, regulation, legal process or governmental request.

This condition, in our view, invites abuses. More attention to detail is necessary. The word “request” implies a potential for omission of the due process that would be required in the EU and in many other countries.

Some clarification is offered in the following clause:

Google may monitor, edit or disclose your personal information, including the content of your emails, if required to do so in order to comply with any valid legal process or governmental request (such as a search warrant, subpoena, statute, or court order), or as otherwise provided in these Terms of Use and the Gmail Privacy Policy.

Note the use of the conjunctive “or”. The word “request” remains undefined. The conditions imposed by US legislation such as the PATRIOT Act could provide a range of opportunities for US agencies to seize content without judicial authority (11)

Additional concerns arise from the following conditions:

Google also reserves the right to access, read, preserve, and disclose any information as it reasonably believes is necessary to (a) satisfy any applicable law, regulation, legal process or governmental request, (b) enforce this Agreement, including investigation of potential violations hereof, (c) detect, prevent, or otherwise address fraud, security or technical issues (including, without limitation, the filtering of spam), (d) respond to user support requests, or (e) protect the rights, property or safety of Google, its users and the public. Google will not be responsible or liable for the exercise or non-exercise of its rights under this Agreement.

This sweeping condition should be contrasted with the view of the Article 29 group:

The content of e-mail has to be kept secret and must not be read either by any intermediary or by the Mail Service Provider, even for so called “network security purposes”. (12)

As noted by the Article 29 Group in its guidelines on privacy & the Internet:

The confidentiality of communications is protected by Article 5 of Directive 97/66/EC. Under this provision, no third party should be allowed to read the contents of e-mail between two parties.

The Article 29 Group provided further elaboration on the question of email interception:

The Article 29 Working Party has dealt with the privacy aspects of interception of communications in its recommendation 2/9956. In this recommendation, the Working Party points out that each interception of telecommunications, defined as a third party acquiring knowledge of the content and/or traffic data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunications services, constitutes a violation of an individual’s right to privacy and of the confidentiality of correspondence. It follows that interceptions are unacceptable unless they fulfill three fundamental criteria, in accordance with Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950⁵⁷, and the European Court of Human Rights’ interpretation of this provision: a legal basis, the need for such a measure in a democratic society, and conformity

with one of the legitimate aims listed in the Convention.

And:

Everyone has the right to send a mail to everybody else without that mail being read by a third party. Article 5 of Directive 97/66/EC, which covers communications and related traffic data for example sent by e-mail, lays down obligations as to the confidentiality of communications. In addition to these obligations, Article 4 of the same directive obliges the providers of telecommunications services to take appropriate technical and organisational measures to safeguard the security of their services and to inform users about a particular risk of a breach of security and any possible remedies, including the costs involved.

The Gmail Terms of Use do not recognise these fundamental rights and conditions, nor do the terms set specific parameters for the reading or interception of email content.

Subject control over data

Data Protection law ensures that an individual will have the ability to control her own data. The following clause indicates that this right may breach the Terms of Use for Gmail:

Accordingly, you agree that you will not copy, reproduce, alter, modify, or create derivative works from the Service. You also agree that you will not use any robot, spider, other automated device, or manual process to monitor, cache, or copy any content from the Service.

One Internet expert has interpreted this to mean:

You can't use a program -- or even a secretary, or a personal plan or habit -- to pull your own email out of the service! If you want to terminate and move your mail elsewhere, you can't extract or keep copies of your own email. (13)

This condition would violate core principles of data protection.

Given the extremely valuable and extensive reserve of communications data that Google wishes its target customers to amass, the following conditions (while not unusual) are unacceptable:

Google may at any time and for any reason terminate the Services, terminate this Agreement, or suspend or terminate your account. In the event of termination, your account will be disabled and you may not be granted access to your account or any files or other content contained in your account although residual copies of information may remain in our system.

The issue of data retention is dealt with below.

Specific data protection issues in the complaint

Searching of email content

The core sniffing and searching function of Gmail gives rise to a range of concerns. The Article 29 Group has observed:

If *sniffing* is carried out at central knots or junctions in the Internet this could allow for large-scale interception and surveillance of e-mail content and/or traffic data by choosing certain characteristics, typically the presence of keywords. *Sniffing*, as a general and exploratory surveillance activity, even if conducted by government agencies, can only be allowed if it is carried out in accordance with the conditions imposed by Article 8 of the European Convention on Human Rights.

Users have come to expect that the content of their emails may be read to detect spam. The Gmail process does not merely extend this function, it takes it into a new context. We believe that the sifting of email content, whether achieved manually or automatically, raises a number of serious data protection concerns.

Indefinite Retention

Gmail's Terms of Use state:

In the event of termination, your account will be disabled and you may not be granted access to your account or any files or other content contained in your account although residual copies of information may remain in our system.

No time frame for the retention of deleted files is mentioned. It is common for email providers to maintain back-up copies to protect against technical failure, though the backup for a system as large as Gmail should operate close to real-time. Nothing in the Terms of Use limit Google's retention of emails to this specific circumstance. As currently stated, the Terms of Use imply that the retention is indefinite.

Article 6 of the Directive states that data should be:

1 (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

The Article 29 Group has observed:

Another privacy risk associated with e-mail is related to the inability of a user to easily and effectively remove an e-mail message that has either been sent or received as the operation of the delete function will not necessarily expunge a mail from the system. It can in that case be relatively easy for another user of the same machine or a system manager in the case of a networked machine to retrieve a message that the original user intended to delete and believes has

been removed from the system. This issue is obviously not confined to e-mail but it is particularly significant in this context. In order to address this issue systems should be designed so that the operation of the delete function actually expunges information from the system.

Confidentiality

Section VIII, article 16 of the Directive (Confidentiality of processing) requires that:

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.

The Gmail Terms of Use are in conflict with this provision.

Third party issues

The Gmail system does not operate within a closed universe. Anyone can communicate with a Gmail customer. The emails of third parties will be subject to the same conditions as those applying to Gmail customers. That is, the email will be scanned and indefinitely retained. This raises a wide spectrum of issues.

Article 14 of the Directive (The data subject's right to object) stipulates:

Member States shall grant the data subject the right:

(a) at least in the cases referred to in [Article 7](#) (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

These conditions cannot be guaranteed by Google. They are even more uncertain for third parties who communicate with a Gmail user.

Article 12 of the Directive has particular application. It stipulates that data should be subject to certain controls:

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

Offshore processing of data

As evidenced by the analysis above, there are grounds for concluding that the processing of data by Google may not achieve the standards required within the EU. Article 25 of Chapter IV of the Directive (Transfer Of Personal Data To Third Countries) states:

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection,

We would like to draw your attention to the Article 29 Working Group paper "*Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*". (14) This document clearly identifies the legal right of the EU to establish criteria for processing of data via non-EU websites.

It should be noted that according to the list provided by the US Department of Commerce, Google has not joined the Safe Harbor scheme. (15) Nor, in our view, has the company satisfied many of the requirements contained in the EU Directive or in the law of EU member states.

Consent issues

Article 7 of the Directive requires that Member States shall provide that personal data may be processed only if the data subject has unambiguously given his consent. This consent, as you will understand, must be given in full knowledge of the circumstances of the processing.

We believe that such informed consent cannot be possible under the current Gmail contract. Customers must be explicitly warned that their data will not be afforded the level of protection that applies in the EU.

It appears that the Gmail service is in material breach of the consent provisions of data protection law. As mentioned above, consent can only be given by a Gmail account-holder. Those who send email to a Gmail customer will have no opportunity to consent to having their email read for keywords.

Sensitive data

Article 8 of the Directive (The processing of special categories of data) stipulates:

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent;

(-)

These provisions raise important and complex questions. To what extent can or should Gmail (or any other email service provider) conform to these requirements? Because of its scale, Gmail can be used by a range of organisations as the primary communications medium.

Conclusion

We believe the Gmail service involves significant and far-reaching privacy implications. The precedent set by the service, its enhanced functionality and the likelihood of unexpected future changes to the system require serious consideration of data protection issues. We urge you to prospectively investigate this system with a view to establishing appropriate privacy safeguards.

Yours sincerely

Simon Davies
Director
Privacy International

References

- 1) Google press release, April 1, 2004
<http://www.google.com/press/pressrel/gmail.html>
- 2) See letter signed by 28 advocates and organisations at
<http://www.privacyrights.org/ar/GmailLetter.htm>
- 3) A selection of coverage can be viewed at
<http://news.google.com/news?q=gmail+privacy&num=30&hl=en&lr=&ie=UTF-8&safe=off&sa=N&tab=nn>
- 4) The text of the Directive can be read at
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

- 5) Four days after the announcement of the Gmail service spymac.com launched a free one gigabyte service
<http://www.spymac.com/news/index.php?contentid=274>
- 6) The UK “Memories for life” research challenge, for example, has proposed a system that would store and index users’ “digital memories” – photographs, videos and communications – over their entire lifetime².
<http://www.csd.abdn.ac.uk/~ereiter/memories.html>
- 7) A snapshot of the ad placement can be seen at
<http://gmail.google.com/gmail/help/screen2.html>
- 8) Edward C Baig, Targeted ads tied to Gmail's super space, USA Today, 14th April 2004.
http://www.usatoday.com/tech/columnist/edwardbaig/2004-04-14-baig_x.htm
- 9) Google’s Privacy Policy
<http://www.google.com/gmail/help/privacy.html>
- 10) Gmail’s Terms of Use
http://www.google.com/gmail/help/terms_of_use.html
- 11) The potential for interference with US based communications services under the provisions of the PATRIOT and other Acts has been the subject of media commentary. See, for example,
<http://www.eurweb.com/articles/columns/04082004/columns1398904082004.cfm> and
<http://www.fortwayne.com/mld/newssentinel/news/editorial/8439289.htm>
- 12) Article 29 Data Protection Working Party; Working Document: Privacy on the Internet- An integrated EU Approach to On-line Data Protection- 5063/00/EN/FINAL WP 37. November 2000
http://europa.eu.int/comm/internal_market/privacy/workinggroup/wp2000/wpdocs00_en.htm
- 13) John Gilmore; assessment of Gmail Terms of Use, 7 April 2004
<http://craphound.com/gilmoreongmail.html>
- 14) ARTICLE 29 - DATA PROTECTION WORKING PARTY
5035/01/EN/Final WP 56 Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites Adopted on 30 May 2002

² Andrew Fitzgibbon and Ehud Reiter. “Memories for life” – managing information over a human lifetime. Grand Challenges in Computing workshop, May 2003. Available from http://www.nesc.ac.uk/esi/events/Grand_Challenges/proposals/Memories.pdf

- 15) US Department of Commerce; Safe Harbor list
<http://web.ita.doc.gov/safeharbor/SHList.nsf/WebPages/Safe+Harbor+List!OpenDocument&Start=175>