SUBMISSION NO. 24

Google Australia Pty Limited
ACN 102 417 032
Level 5
48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

30 June 2009

The Secretary
House of Representatives Standing Committee on Communications
R1-109
Parliament House
coms.reps@aph.gov.au

Inquiry into Cyber Crime

We thank the House of Representatives Standing Committee on Communications (Committee) for its letter to Mr Chad Hurley, CEO of YouTube, of 1 June 2009 and appreciate the opportunity to provide comments as part of the Committee's inquiry into cyber crime.

This submission is made on behalf of Google and YouTube. Google, through acquisition, is also the provider of the well-known YouTube service.

Google's breakthrough technology and continued innovation serve our mission of 'organising the world's information and making it universally accessible and useful.'

Google spends a lot of time developing new products that assist users. Google also spends a lot of time working on the security aspects of those products. We take our responsibility to protect users' security seriously and we recognise that secure products are instrumental in maintaining users' trust.

Based on our experience, we believe that service providers are motivated to work towards a safe and secure environment for their users as this is fundamental to obtaining and maintaining users' trust – which is key to success. In order for a service to be successful, users must feel comfortable using the service. Providers want their brand associated with comfort, safety and security. Ultimately, it is imperative to providers' bottom line to get e-security risk-management right.

In the online environment there is a vast array of service providers, providing a diverse range of online services. Each of these services use a variety of technological tools to mitigate e-security risks – the same tools will not work effectively in all services. Further, new technological tools are constantly being developed – we are seeing breakthrough technologies emerging in the space of months.

In this submission we provide an overview of key measures currently deployed by Google and YouTube to mitigate e-security risks faced by Australian consumers. In particular we outline:

- Google's activities and the power of the open Internet
- Google's security philosophy
- Google's provision of security services

Google Australia Pty Limited
ACN 102 417 032
Level 5
48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

- how Google empowers users with information
- technological tools on YouTube that mitigate e-security risks, including its partnerships with law enforcement.

About Google

Google initially became familiar to most Internet users as the provider of the Google search engine and subsequently as the provider of email, instant messaging and specialist search and information services, including Google News and Google Finance.

Google Maps is another specialist information service that has become incredibly widely used. It's a little-known fact that Google Maps was invented in Australia by four engineers. The team had a vision that maps could be used as a dynamic platform for geospatial services - that local businesses, restaurants, movies could all be visualised online. Most people who use the web will encounter the Australian-born phenomenon that is Google Maps. Australian local businesses, satellite views and driving directions are all integrated into the product. It's also the basis of thousands of 'mashup' websites, including real estate websites, travel publications and restaurant guides.

Google, by acquisition of YouTube, is also the provider of the well-known YouTube service. Google and YouTube are not social networking services however there are social elements to our video sharing platform YouTube. YouTube is a user generated video sharing platform around which communities form, have discussion and interact.

Google operates a major research and development centre in Australia. Google's Australia research and development team, which includes the key engineers who created Google Maps, works on global products that are making a positive difference in tens of millions of lives every day. This is most recently demonstrated by the launch of Google Wave for developer preview. Google Wave is a new tool for communication and collaboration on the web. It is currently in an early developer preview stage and we expect to open the service more broadly later this year.

In addition, Google serves Government and corporate clients, including advertisers and content publishers, with cost-effective advertising and a wide range of search services.

Google Apps is a hosted messaging and collaboration platform – a set of applications and tools that enables Government and corporate clients to deploy leading technologies for their users in a cost effective way. Google Apps demonstrates Google's commitment to being a leader in the provision of innovative collaboration and communication products.

The power of the open Internet

The Internet has had an enormous impact on people's lives around the world. It has changed entertainment, culture, business, health care, the environment and more. The Internet has democratised the creation and dissemination of information, with huge opportunities for free expression.

The Internet is an open environment, it allows 'innovation without permission': any user can create and offer applications or content to all other users, and users themselves are in control of what content and applications they access.

Google Australia Pty Limited
ACN 102 417 032
Level 5
48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

Access to the open Internet enables Australians to fully engage in the global digital economy and Australian businesses to more effectively compete on the world stage. In the open Internet, alternative services are only ever a click away and the only way to succeed is to provide superior services, through constant technological improvement, innovation and focussing on earning users' trust.

Google's security philosophy

Google spends a lot of time developing new products that assist users. Google also spends a lot of time working on the security aspects of those products. We take our responsibility to protect users' security very seriously and we recognise that secure products are instrumental in maintaining users' trust.

Google treats security as a continuous process. We consider the security requirements and features of a product from the time the product idea is conceived throughout the product's development and life.

Google strongly believes in layered protection. We believe that this is much like securing your house. You put your most private information in a safe, which is secured in your house, which is protected with locks and possibly an alarm system. Then you also have neighborhood watch and local police monitoring your neighborhood. We implement this philosophy as follows:

- At Google, the most sensitive information is difficult to find or access. Our network and facilities are protected in both high-tech and low-tech ways: encryption, alarms and other technology for our systems; and strong physical security at our facilities.
- We have learned that security is enhanced by taking an industry-wide approach. We encourage everyone to help us identify potential problems and solutions. Researchers who work at security and technology companies all over the world are constantly looking for security problems on the Internet and we work closely with that community to find and fix potential problems.
- Google also invites its user community to be involved in this process. Google's users are able to report security concerns, which may relate to password problems, login issues, spam reports, suspected fraud, account abuse, suspected vulnerabilities in Google products or security incidents. Google responds swiftly to fix security issues. These combined efforts go a long way in making the Internet safer and more secure.

These layers of protection are built on excellent security technology. Google uses both products developed by others in the security community and our own security technologies. Some of the most innovative components of our security architecture focus on automation and scale. These are important because we are handling searches, emails and other activities for millions of users every day. To keep our security processes a step ahead, we automate the way we test our software for possible security vulnerabilities and the way we monitor for possible security attacks. We are also constantly seeking more ways to use encryption and other technical measures to protect data, while still maintaining a great user experience.

In addition to technology, we have a set of processes that dictate how we secure confidential information at Google and who can access it. We carefully manage access to confidential information of any sort and very few Google employees have access to what we consider

Google Australia Pty Limited
ACN 102 417 032
Level 5
48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

very sensitive data. Partly, this is because there is very little reason to provide that access - most of Google's processes are automated and don't require much human intervention. Of course, the limited number of people who are granted access to sensitive data must have special approval.

Google also works to ensure that its processes meet (and in many cases exceed) industry standards. By working with independent auditors, who evaluate compliance with standards that hold hundreds of different companies to very rigorous requirements, we add another layer of checks and balances to our security processes.

In addition to this, we employ exceptional Google security engineers. Many of our engineers have come from very high-profile security environments, such as banks, credit card companies and high-volume retail organisations, and a large number of them hold PhDs and patents in security and software engineering.

Google's engineers are smart, curious and on the lookout for security anomalies and best practices in the industry. We also cultivate a collaborative approach among all of our engineers, requiring everyone to pass a coding style review (which enables us to control the type of code used and how it's used in order to prevent software problems) and ensuring that all code at Google is reviewed by multiple engineers so that it meets our software and security standards.

While we continue to innovate with our products, we also continue to innovate in the world of security.

Google's provision of security services

Google offers security services to our users as part of our Google Apps offering.

Google Apps leverages Google's extensive, secure, global infrastructure to provide clients an entirely hosted solution for email, document management and more. Google manages the data and software for the client, eliminating the costly overheads of storage, hardware and software maintenance, spam and security.

Google Apps Security Services are powered by Postini and provide a client with spam, virus filtering, email filtering, encryption, email archiving and web security. These services help an organisation to be more secure, compliant and productive, using its existing email infrastructure. As a service, there is nothing to install or maintain. Service packages are available at different levels and price points, so there is something to meet everyone's needs.

How Google empowers users

Google has deployed extensive resources to educate and empower users.

Google offers all Australians a free collection of software which contains Norton Security Scan and Spyware Doctor Starter Edition, to detect and remove viruses, worms, spyware, adware, trojans and keyloggers.[1]

[1] This is available at http://pack.google.com/intl/en-gb/pack_installer.html?hl=en-gb&gl=au),

Google Australia Pty Limited
ACN 102 417 032
Level 5
48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

Google believes in providing users with information about safe web practices. This includes:

- In conjunction with Stop Badware.org, we place warnings in our search results for websites that our testing has determined to host or distribute badware. If you search for a site that Google has determined to be potentially dangerous, you will see a warning in the search results.[2]
- The Google Online Security Blog,[3] including the following posts:
  - Announcing "Browser Security Handbook"[4]
  - Malware? We don't need no stinking malware![5]
- Blog postings on Google's Official Blog, for example:
  - Does your password pass the test?[6]
  - How to avoid getting hooked[7]
  - Working together to fight malware[8]
- Useful information within the Google Help Centre[9]
- YouTube videos on secure practices, such as: 'To keep your gmail account secure'[10]
- Information within specific product help and safety centres, such as the YouTube Safety Centre.[11] The YouTube Safety Centre contains localised Australian information for users including advice on privacy, tips on how to be responsible cyber citizens and how to use the community flagging system. We have partnered with Australian organisations to provide this information including the Australian Communications and Media Authority, the Australian Federal Police, Bravehearts, Kids Helpline and Reach Out.
- Partnering with government initiatives in cyber-safety, such as supporting the Government's National eSecurity Awareness Week.[12]

We also believe in harnessing our own products, technology and resources to help partners deliver relevant and useful information (advertising) to users worldwide. Promoting safer and more secure internet experiences for users is an important part of our efforts in this regard. The Google Grants program uses the power of the Internet to help nonprofit organisations to inform, engage and connect with users online.[13]

---

[2] For more information, see http://www.google.com/support/websearch/bin/answer.py?answer=45449
[3] Available at http://googleonlinesecurity.blogspot.com/
[4] http://googleonlinesecurity.blogspot.com/2008/12/announcing-browser-security-handbook.html
[5] http://googleonlinesecurity.blogspot.com/2008/10/malware-we-dont-need-no-stinking.html
[6] http://googleblog.blogspot.com/2008/06/does-your-password-pass-test.html
[7] http://googleblog.blogspot.com/2008/04/how-to-avoid-getting-hooked.html
[8] http://googleblog.blogspot.com/2008/04/working-together-to-fight-malware.html
[9] For example http://mail.google.com/support/bin/answer.py?hl=en&answer=29409
[10] http://www.youtube.com/watch?v=6UzYo8yf0Uo&feature=user
[11] Available at http://help.youtube.com/support/youtube/bin/request.py?contact_type=abuse&hl=en-GB
[12] See http://google-au.blogspot.com/2009/06/supporting-national-e-security.html
[13] For more information, see http://www.google.com.au/grants/

Google Australia Pty Limited
ACN 102 417 032
Level 5
48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

Technological tools on YouTube that mitigate e-security risks

The Committee's letter to Mr Chad Hurley, CEO of YouTube, of 1 June 2009 asked how social networking sites protect user information. YouTube is not a social networking service however there are social elements to it. In this section we provide some material which looks specifically at how cyber-security issues are handled for YouTube.

YouTube is a user-generated video sharing platform around which communities form, have discussion and interact. Every minute, 20 hours of video are uploaded to YouTube. As a platform for user-generated content, and given the volume of content, it is not possible to review videos in advance of them being made available on the site.

The primary security and safety features on YouTube are as follows:

- The YouTube Community Guidelines (http://au.youtube.com/t/community_guidelines) set out what is, and is not, acceptable - for example adult content, graphic violence, hate speech, harassment, invading privacy, or the revealing of other peoples personal information is not allowed. Users who repeatedly violate guidelines have their accounts terminated.
- YouTube has developed an innovative, reliable and user-friendly community policing system - users report potential violations of the YouTube Community Guidelines by "flagging" a video, flagged videos are then reviewed for compliance with the Community Guidelines 24 hours a day, seven days a week.
- Our YouTube review teams receive extensive training on an ongoing basis, including from law enforcement organisations and child safety organisations. This training enables our team to effectively and efficiently respond to flagged videos.
- Where a video does not comply with the Community Guidelines, it will be removed from the site and, in appropriate circumstances, referred to law enforcement.
- YouTube has also developed digital hashing technologies to prevent the re-upload of files that have been removed, and is continually developing tools to promote this goal.
- In addition to the flagging system, users are able to contact YouTube directly with privacy, harassment, or bullying complaints through the Help & Safety Tool.

Users are also empowered to manage their own experience by:

- uploading videos as "Private" to be shared with specified family and friends
- blocking specific users from interacting with them
- choosing to allow only their "friends" to communicate with them
- choosing to pre-screen comments
- choosing to disable commenting altogether for each of their videos
- choosing to filter the comments they see. This is a new feature that has resulted from YouTube engineers' constant innovation. Filter W*rds gives users the control to set their preferences so that they see only filtered comments.

In relation to privacy concerns, the YouTube Community Guidelines state:

Google Australia Pty Limited
ACN 102 417 032
Level 5
48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

> "There is zero tolerance for predatory behaviour, stalking, threats, harassment, invading privacy, or the revealing of other members' personal information. Anyone caught doing these things may be permanently banned from YouTube. … Violations of the Terms of Use may result in a warning notification or termination of your account. If your account is terminated you are prohibited from creating any new accounts."

Where these types of concerns arise we typically remove a video or comments if personally identifying information is disclosed. We will also typically remove a video if an individual complainant is clearly identifiable in a video and their permission has not been obtained.

Conclusion

Working towards our users' online safety and security is a key priority for Google and YouTube. Providing a safe and secure environment for users is fundamental to obtaining and maintaining users' trust – which is the key to success. The vast array of online services that are available provide wonderful opportunities and benefits which it is important that all Australians have the opportunity to enjoy.

We look forward to following the work of the Committee as it considers the important issues captured within its Terms of Reference.

Kind regards

Ishtar Vij
Public Policy and Government Affairs Manager
Google Australia and New Zealand