



**Australian
Privacy
Foundation**

<http://www.privacy.org.au>

Secretary@privacy.org.au

<http://www.privacy.org.au/About/Contacts.html>

The Committee Secretary
House of Representatives Standing Committee on Infrastructure and Communications
PO Box 6021
Parliament House
Canberra ACT 2600
Via email: ic.reps@aph.gov.au

Dear Committee Secretary,

Re: Inquiry into the use of s.313 of the Telecommunications Act

Thank you for the opportunity to make a submission to this Inquiry. This submission is made by the Australian Privacy Foundation Inc, the country's leading privacy advocacy association. A brief backgrounder relating to the APF is attached.

The terms of reference of the Inquiry relate to government agency use of section 313 for the purpose of disrupting illegal online services.

The Committee is to consider:

(a) which government agencies should be permitted to make requests pursuant to section 313 to disrupt online services potentially in breach of Australian law from providing these services to Australians;

(b) what level of authority should such agencies have in order to make such a request;

(c) the characteristics of illegal or potentially illegal online services which should be subject to such requests; and

(d) what are the most appropriate transparency and accountability measures that should accompany such requests, taking into account the nature of the online service being dealt with, and what is the best/appropriate method for implementing such measures:

a. Legislation

b. Regulations, or

c. Government policy.

Other submissions may well focus on the problems with Government agencies making semi-qualified assessments of the illegality of websites, and then shutting them down without any court

order. These are not the behaviours of a country subject to the rule of law. However, this submission wishes to focus on the extremely adverse impact on Australians' privacy that the continuing misuse of section 313 will have; and the folly of creating a system which collects private web-browsing information.

Section 313 is in reality not one single provision but multiple disparate provisions, considered from the perspective of (a) whether or not any event has taken place and (b) the degree of obligation to respond to directions.

For example, in relation to "Crime Prevention (Australian offences) ss.313(1) and (2)" do not require the commission of an offence nor have penalties for non-compliance. However with "Law Enforcement (Offence of any country, and fines etc.) ss.313(3) and (4)" - typically an offence has occurred or is happening, evidence is required and there is an obligation to comply with reasonable requests. With the sections on "Safeguard National Security ss.313(3)(e), (4)(e)" - the offences under scrutiny are often preventative, but there is an obligation to comply with requests. ISPs may be forgiven, if not excused, for dealing with all requests under s.313 in the same obedient manner irrespective of the source of the power to request information, or even the type, sensitivity and intrusiveness of the information requested. From a privacy perspective, there is a considerable difference between the proportionality of the information requests and the types of information based on the source of power to demand/request information and the nature of the agency requesting the information.

Ignoring for the moment the genuine doubts that any Government agencies should be empowered to be judge, jury and executioner of a website; the method of operation of takedowns under complex and overlapping provision of s.313 is unnecessarily damaging to privacy interests in a way contrary to the proportionality requirements of the collection of private information under the Privacy Act. Inter alia, the offending conduct arises from:

- Agencies monitoring and collecting personal information including interactions with websites without reference to either party to the communications;
- The term "assisting in any way" is interpreted by agencies or ISPs as a duty to store and render client information beyond so-called "metadata". Telstra has recently admitted applying the law in this fashion.
- Storing such information with risk of leaks, loss and breach;
- Making defamatory representations to web hosts, domain registrars and others utilising private information to obtain client information;
- Creating at web hosts the "Taken Down" webpage which can result in effortless storage of the IP addresses of anyone subsequently attempting to access that page. This list of unsuccessful

attempts is – of course – a highly sensitive document capable of being misused by Government or criminals;

- Mission creep is a real concern – without a definition of “serious crime”, websites anywhere in the world, offending anyone anytime, could be subject to takedown with all the attendant privacy concerns. Last year, in a written submission to the Senate Economics Legislation Committee, ASIC admitted – without apology – that it caused to be blocked 250,000 websites by mistake. You may be aware that ACMA has over-blocked on spurious law-enforcement grounds or simply by bureaucratic mistake. Blocklists are difficult to compile and keep up to date and so far no Government worldwide has successfully managed these complicated tasks. While ACMA is relatively skilled and staffed for the task of website takedowns, it is highly unlikely that other agencies have the practical skills, training or experience with diversity to take on the task of pre-emptive crime-stoppers.
- If a website is taken down, visitors to the site suffer two hazards – their visit to the site address is trackable and if they wish to complain their personal information must be revealed to do so. These new privacy intrusions are unacceptable.
- There are already takedown powers granted to ACMA, and a separate Act relating to telecommunications intercepts. What purpose remains in s.313 other than unaccountable bureaucratic discretion?
- Section 313 and any demands thereunder have the potential for being a second vector for agencies to quasi-lawfully access telecommunications data – for example requiring an ISP to keep the personal information the Government likes to reference as “metadata” without lawful process, or to track access to the front-end or back-end of the website. A broad requirement to store and render “all data connected with this account” would be comprehensive and compromise the privacy of the account holder and all who access the Internet via that account.

- Serious crimes are already adequately dealt with by financial regulations, CERT and laws of general application including injunctive relief and third-party orders. There is no “gap” for any agency with a legislative function to takedown websites on its own woolly-headed motion.
- If a website is blocked pursuant to s.313, at minimum there should be notification to the site owner and an avenue of review and/or appeal. The privacy issues with appeals should be noted as especially problematic, given the normal transparency of statutory appeals.

Accordingly, in the Foundation’s submission:

(a) No government agencies should be permitted to make requests pursuant to section 313 to **disrupt online services** potentially in breach of Australian law from providing these services to Australians. This is a task for law-enforcement and the Courts on application from the agencies as expert on the facts at issue. Our research does not disclose any time s.313 has been the subject of review or control by the Courts, giving rise to a perception that the present behaviours of Government agencies are of dubious legality, unchecked in fact and unsupported by legislation applicable to those agencies. Currently requests to ISPs by agencies are not even publicly recorded, let alone monitored for compliance with the laws including the Privacy Act.

(b) There is no level of authority with adequate safeguards for the public interest for either takedowns or use of s.313 to require ISPs to render personal information as agencies are not qualified to assess these matters. Their governance and sponsorships imbue bias and bad faith in decisions already manifest under the shadowy rules agencies assert at present. There is a difference between “law enforcement” and “crime prevention”; and the latter may affect websites that are wholly legal. The insertion of s.313.3(ca) to require ISPs to assist the Government to take down websites that are illegal under foreign laws (but not our own) is especially troubling.

(c) The characteristics of illegal or potentially illegal online services which should be subject to such disruptions or requests for “assistance” are the same as crime, and should be dealt with by law-enforcement and Courts. It is unrealistic to assume that senior officers in Government agencies will ever be adequately trained to make these decisions, and on the contrary the trend is towards automatic systems which will further over-block. Under s.313(1), there is no legal requirement to comply with a request from a Government agency; but the unrelated compulsions under s.313(3), and a reluctance to antagonize authorities, may have encouraged ISPs in the past to behave as if there is a need to do what they are told, in secret and without due process. This has been partly responsible for creating the de facto Australian model for non-transparent ‘mandatory’ censorship of websites for crime prevention purposes, when any action taken by the carrier/CSP is misleadingly described as voluntary and unconscionably incapable of protest by the end-user. An expanded use of s.313(3)(e) "safeguarding national security" as a new, third limb of unauthorized censorship and information gathering under the Act would invite any sort of Government over-reach, including shutting down whistle-blower websites for political reasons

(since in that section there's no need for there to be a criminal or civil offence to trigger the unlimited "national security" claim).

(d) The most appropriate transparency and accountability measures that should accompany such requests must be the Courts, even for very serious offences and perhaps more so for trivial matters which be prosecuted by agencies in bad faith under political pressure. It follows that any takedown regime which the Government genuinely believes is required over and above the existing, ample, laws of general application are subject to the same minimum standards under legislation of due process, proper notice, right to be heard, right of appeal and right of an open Court. It should go without saying that such powers to takedown websites are not a proper subject for Government policies. The parliament of Australia does not support an extension of the Broadcasting Services Act to allow Government the power to have ISP filtering of websites; it would be iniquitous if the quietly expanded use of s.313 was abused to evade Parliament's objections. At present, an agency could misuse s.3.13 to require Telstra to cut off a whole country, or a whole web host company, or anyone who has aggrieved a junior officer, without recourse or appeal. Only clear and definite legislation defining the process and the civil rights of those affected can be conscionable in a democracy.

We submit that s.313 should be wholly re-written to establish due process and appeal rights, to remove conflicts and confusion between the diverse subject matter comprising "law enforcement" "crime prevention" and "national security" and include a definition of "serious crime" by reference to statutes covered or penalty points upon conviction. Otherwise we can expect a zealous library clerk to use s.313 to seek takedown of book review sites as inspiring or instructing the offence of having overdue library books.

While the subject-matter of this Inquiry is new, the principles of proportionality and democratic control of State Surveillance are not new. The Foundation has previously written on these topics – online at the APF website (and annexed for convenience):

Meta-Principles for Privacy Protection: <http://www.privacy.org.au/Papers/PS-MetaP.html>

Policy Statement on Democratic Control of Surveillance by the State:

<http://www.privacy.org.au/Papers/PS-SS.html> - an essential part of which is "all powers must be exercised transparently, and must be subject to effective controls, audit, oversight, complaints-handling, investigation, sanctions and enforcement".

For example, another issue relevant to proportionality is the ss.313(5) and (6) immunity applying to actions done for s.313(1) prevention, (noting all those mistaken domain blockings in recent examples). Leaving victims without a remedy against negligent damage to business, security compromise, breach of confidentiality, or privacy intrusion is outrageous when it is for unsupervised s.313(1) crime prevention, since s.313(1) crime prevention actions are often open-ended and essentially speculative, are not restricted to actions "reasonably necessary", and there

is no enforceable obligation on ISPs to account for their view on what "doing your best" is. The immunity is a disincentive to caution, due process and respect for consumer rights.

The Inquiry may wish to examine the use of s.313 requests and subject the same to analysis as to the usefulness and proportionality of the requests to date. Are destination IP addresses being collected now, against all promises – noting the strong opinion of Internet expert [Geoff Huston](#) that metadata retention must necessarily lead to logging of all user traffic.

Technical issues should be seriously considered by the Inquiry. Many Australians protect their privacy, as they are entitled to do, by use of Virtual Private Networks and similar activity-masking technologies. Just as with Internet censorship, if the Government wants to examine people's access to the Internet it will have to break encryption, including widely-used online banking technologies. The more the Australian Government departs from international norms, the more Australians will use VPNs to mask their Internet activities and this may well contribute to the proliferation and growth of websites hidden behind masking technologies such as The Onion Router (TOR). If compliance with s.313 is only enforceable against users tied to 20th Century technologies, the incentive will be to use software to evade the law. The law may be undone by a software update.

Let's not have the worst of both worlds – where the technologically savvy evade clumsy laws administered by amateurs; but ordinary Australians running websites are liable to be shut down by any bureaucrat with a badge and traffic to and from those sites is mined by Government with organized crime as the unintended beneficiaries.

For and on behalf of the Australian Privacy Foundation,

Kimberley Heitman, B.Juris, LLB, MACS, CT,

Board Member

22nd August 2014

Australian Privacy Foundation - Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organizations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organizations who support the APF's Objects. Funding that is provided by members and donors are used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, Subcommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, Subcommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby AC CMG and The Hon Elizabeth Evatt AC, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies <http://www.privacy.org.au/Papers/>
- Resources <http://www.privacy.org.au/Resources/>
- Media <http://www.privacy.org.au/Media/>
- Current Board Members <http://www.privacy.org.au/About/Contacts.html>
- Patron and Advisory Panel <http://www.privacy.org.au/About/AdvisoryPanel.html>

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) <http://www.privacy.org.au/About/Formation.html>
- Credit Reporting (1988-90) <http://www.privacy.org.au/Campaigns/CreditRpting/>
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- The Media (2007-) <http://www.privacy.org.au/Campaigns/Media/>