Submission to the Australian Government Discussion Paper

Strengthening Australia's cyber security regulations and incentives

SEPTEMBER 2021

FACEBOOK

Executive summary

Facebook welcomes the opportunity to provide a submission in response to the Australian Department of Home Affairs' consultation on proposed new cyber security regulation.

Combatting cyber security threats is a continuous challenge. It requires governments, industry and individuals to each play their role and adapt to changing circumstances. We all have a shared interest in ensuring a strong cyber security ecosystem in Australia, and the actions and cyber security of one actor can have a broader effect on the cyber security of others.

Facebook takes the challenge seriously and we have invested significantly over a long period of time to play our part. We now have more than 35,000 people working on safety and security across the company. We also have a number of relevant cyber security initiatives already in place, including policies and enforcement to stop malicious behaviour, a sophisticated bug bounty program, a policy for disclosing vulnerabilities of third parties, and tools and regular education to empower users.

We welcome this consultation process as an opportunity to discuss how the Australian Government and industry can collaborate to improve cyber security. The best way to meet our cyber security challenges is to incentivise collaboration and encourage best practice between the various players involved in protecting cyber security.

Regulation can play a role: there is already Australian regulation relating to cyber security (including under privacy legislation that is being reviewed). However, there are some inherent aspects of regulation that may make it less suitable for encouraging collaboration and best practice on cyber security. As the discussion paper correctly identifies, regulation can encourage a compliance mindset (focussing on "ticking the boxes"), which is less effective than a mindset of continuous improvement.

It is also important to ensure that regulation does not set prescriptive requirements that can become quickly outdated as threats and technology adapt. Regulation should be careful to ensure penalties are borne by the bad actors who perpetrate cyber security threats - not the companies that find themselves under attack.

For these reasons, we believe this consultation process presents an opportunity to encourage greater collaboration between governments and industry to combat threats. We are supportive of approaches that involve voluntary governance standards, greater regulatory guidance about expectations for managing user data, and encouraging

voluntary uptake of responsible disclosure policies - all in close collaboration with industry.

We also recommend the Australian Government take a holistic approach to cyber security. Proposals around amending the Privacy Act and Australian Consumer Law are already being considered by separate current inquiries, and we recommend allowing those processes to run their course first. Similarly, there appear to be divergent approaches across the Australian Government to issues like encryption, and we suggest a consistent approach is adopted across government on this issue.

We welcome the chance to collaborate further with the Australian Government and broader industry on how best to enhance the cyber security of Australians. Facebook is planning additional work to support small businesses to enhance their cyber security, and we would be very happy to work with the Department of Home Affairs on how we can work together in this regard.

Summary of Facebook's submission

Government proposal		Summary of Facebook's response
Setting clear minimum expectations	Governance standards for large businesses	We **support** voluntary cyber security governance standards, drafted in consultation with industry.
	Minimum standards for personal information	We **support** the Government's intention to provide greater guidance for businesses on ways to manage personal information. However, we suggest this is achieved through voluntary guidance on expectations issued by the Office of the Australian Information Commissioner rather than via a regulatory code under the Privacy Act. This would help to avoid duplication with the review of the Privacy Act (including the principle around user security) that is currently underway.
	Standards for smart devices	We **support** standards for smart devices, to the extent they are harmonised with relevant international standards, and are voluntary for businesses to adopt in the first instance.
Increase transparency and disclosure	Labelling for smart devices	We **have concerns** about mandatory labelling schemes at this stage, given the lack of clarity around whether labelling schemes are effective for cyber security and how to implement them. We note the Government itself raises concerns that there is insufficient data about the effectiveness of labelling schemes, and we suggest the Government waits until there is data on the effectiveness of schemes in other jurisdictions (such as the pilot scheme in the US, or the new scheme in the UK).
	Responsible disclosure policies	We **encourage** the Government to work with industry to see what can be achieved via voluntary uptake of responsible disclosure policies, before mandating a particular approach. As an industry leader in this space, Facebook would welcome the opportunity to share more about our approach.
	Health checks for small businesses	**No comment**. Given we would not be subject to the proposals relating to small businesses, we have no comment on these proposals.

Protecting consumers	Remedies to consumers under Australian Consumer Law	We **do not support** changes to the Australian Consumer Law (ACL), given the ACL already provides recourse for practices that are misleading or inadequate and offers protections to consumers covering a wide variety of consumer products, including in the digital space.
	Direct Right of Action through the Privacy Act	We **suggest** any changes to the Privacy Act should be considered via the inquiry currently underway and led by the Attorney-General's Department, rather than via this process. This will help to ensure any privacy changes are aligned with the overall legislation. We have already raised concerns through the existing review of the Privacy Act about how a direct right of action could impact court resources.

Table of contents

Facebook's work on cyber security

Facebook is committed to playing our part to protect the security of our users. Cyber security is in everyone's interest.

We have significantly increased our commitments and investments in this area in recent years, and we now have 35,000 people working on safety and security within Facebook.

We take a multi-faceted approach to cyber security, focussing on areas as diverse as penetration testing, spam prevention, disrupting operations run by adversaries (such as cyber espionage, foreign interference or hacking), data protection, and taking legal steps to respond to cyber attacks. We use a combination of expert teams and automated technology to detect potential abuses of our services.

Below, we provide more detail below on:

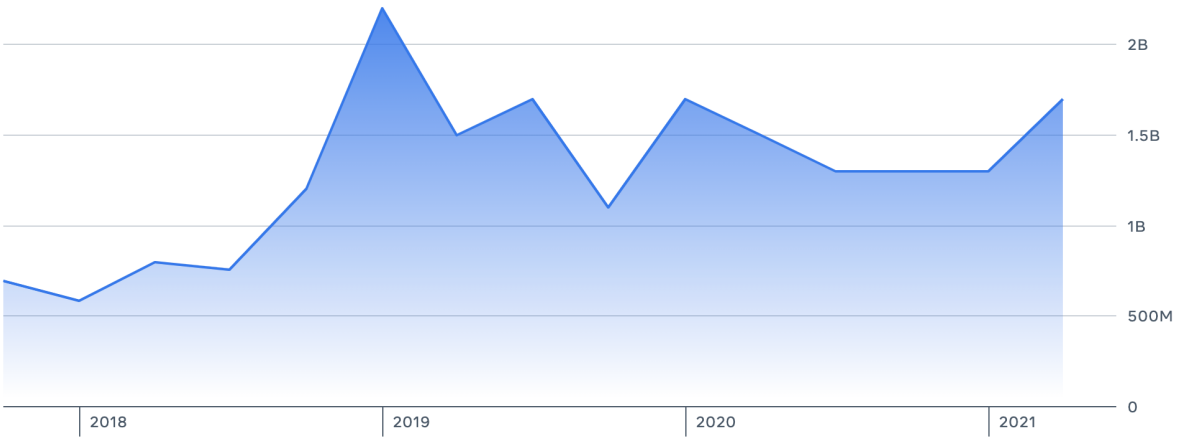
- The **policies** we set for use of our apps and how we **enforce** those policies.
- **Tools** we provide to support Australians to protect their cyber security.
- **Partnerships** to encourage collaboration across the cyber security environment.

Policies and enforcement

Our Community Standards[1], which outline what material is and is not allowed on Facebook, prohibit inauthentic accounts or behaviour that intends to mislead users. Specifically, our Community Standards contain requirements about:

- **Authentic identity.** We do not allow fake accounts on Facebook, as they can be vehicles for a range of harmful content and behaviour, including cyber security risks. In the second quarter of 2021, we detected and removed 1.7 billion fake accounts, 99.8 per cent of which we detected proactively[2]. The majority are caught within minutes of registration.

# of fake accounts we've taken action on (2018-2021)

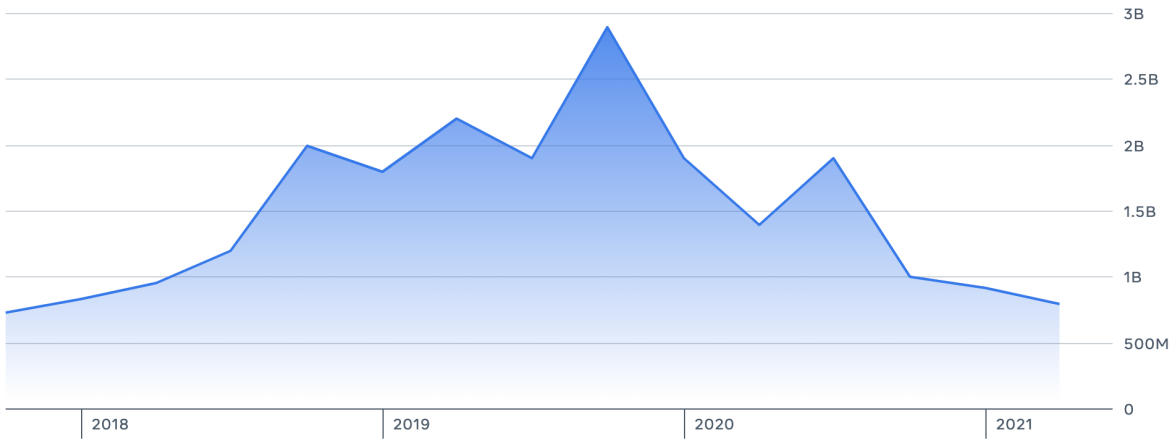


We consider authentic communications to be a central part of people's experience on Facebook. People find value in connecting with their friends and family, and they also find value in receiving updates from the Pages and organisations that they choose to follow. For this reason, authenticity has long been a requirement of our Community Standards. Specifically, our policies prohibit people engaging in inauthentic behaviour, which includes creating, managing, or otherwise perpetuating accounts that are fake, accounts that have fake names, and accounts that participate in, or claim to engage in, coordinated inauthentic behaviour.

[1] Facebook, *Community Standards,* https://www.facebook.com/communitystandards/introduction
[2] Facebook, *Community Standards Enforcement Report Q2 2021,* https://transparency.fb.com/data/community-standards-enforcement/

- **Spam.** We work hard to limit spam on our services. It can threaten the stability or security of our services, and create a poor experience for users. In the second quarter of 2021, we took action against 794 million pieces of spam content, 99.7 per cent of which we detected proactively.

# of pieces of spam content we have actioned (2018-2021)



- **Cybersecurity.** We specifically have a policy that users cannot: attempt to compromise user accounts, profiles or other Facebook entities; attempt to gain authorised access; gather sensitive information via deceptive means; or abuse our products and services. In particular, we do not allow:
    - encouraging or deceiving users to download or run files or programs that will compromise their online or data security (such as malware),
    - attempting to obtain, acquire or request another user's login credentials or other sensitive information, whether explicitly, through deceptive means (like phishing) or the use of malicious software or websites,
    - publicly sharing your own or others' login information, either on our platform or through a third party service,
    - creating, sharing or hosting malicious software, whether on or off the platform, and
    - providing online infrastructure, including web hosting services, domain name system servers and ad networks that enable abusive links such that a majority of those links on our services violate the spam or cybersecurity sections of the Community Standards.

- **Inauthentic behaviour.** In line with our commitment to authenticity, we don't allow people to misrepresent themselves on Facebook. This policy is intended to protect the security of user accounts and our services, and create a space where people can trust the people and communities they interact with.

There are a number of cyber security threats that have recently originated where we have taken action to protect Australians:

- One such example is the actions we took in March 2021 against a group of hackers in China known in the security industry as Earth Empusa or Evil Eye[3] who targeted the Uyghur diaspora in a number of countries, including Australia. Through a combination of our security and detection measures, we were able to identify a number of cyber espionage tactics and ultimately disrupt their ability to use their infrastructure to abuse our platform, distribute malware and hack people's accounts across the internet. In announcing our detection of this network, we also shared threat indicators - such as malware hashes and malicious domains used - to enable other companies and platforms to detect and stop this activity.

- We have put in place a number of measures to prevent unauthorised scraping of personal data from our platform. These include setting up a new External Data Misuse (EDM) team made up of more than 100 people who focus on detecting, blocking and deterring scraping. We have also introduced rate limits and data limits to restrict how much data a single person can obtain, and we use our technology to look for patterns in activity and behaviour that are typically associated with automated scraping behaviour. Because scrapers' tactics continue to evolve, we regularly review and update our defenses to try to stay ahead of them.[4]

We also take a comprehensive approach to detecting and fixing bugs and vulnerabilities. Our approach includes secure frameworks, automated testing tools, peer and design reviews, threat modeling exercises, and our bug bounty program.

External security researchers are key partners for us. Since 2011, we have encouraged security researchers to responsibly disclose potential issues so we can fix the bugs, publicly recognise their work and pay them a bounty. Our Bug Bounty program has been instrumental in this area. To date more than 50,000 researchers have joined the program

[3] M Dvilyanski and N Gleicher, 'Taking Action Against Hackers in China, *Facebook Newsroom,* 24 March 2021, https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/
[4] M Clark, 'How We Combat Scraping', *Facebook Newsroom,* 15 April 2021, https://about.fb.com/news/2021/04/how-we-combat-scraping/

and we have awarded over $9 million to 1,500 researchers across 107 countries for helping us protect our users, products and services.[5]

Facebook has now expanded the Bug Bounty program to cover all of our web and mobile clients across our family of apps, including Instagram, WhatsApp, Oculus, Workplace and more. As the threat landscape has evolved, we have continued to develop the Bug Bounty program by:

- Providing new, innovative ways to incentivise security research into emerging risk areas, such as the misuse of Facebook data,
- Building new tools to reward the research community such as our Hacker Plus program (which provides rewards to those who help us identify security vulnerabilities), and
- Creating new opportunities for collaboration and networking at live hacking events and BountyCon, a conference for researchers in our bug bounty program.

We may also occasionally find critical security bugs or vulnerabilities in third-party code or systems when we interact with them. In some instances, there may be significant complexity in working through how to resolve the bug with the partner. We have a Vulnerability Disclosure Policy[6] that sets out how we approach these situations. In general, we contact the responsible party as soon as reasonably possible, and we reserve the right to publicly disclose the vulnerability if we do not hear back within a reasonable amount of time. We prioritise the highest risk vulnerabilities. Our priority is to see these issues promptly fixed, while making sure that people impacted are informed so that they can protect themselves by deploying a patch or updating their systems.

We also use legal recourse against those who violate our policies to perpetrate cyber security risks. In the past year, we've taken over 300 enforcement actions against people who abused our platforms.[7] These actions can include sending cease and desist letters, disabling accounts, filing lawsuits or requesting assistance from hosting providers to have accounts taken down.[8]

---

[5] D Gurfinkel, 'Marketing the 10th Anniversary of Our Bug Bounty Program', *Facebook Newsroom*, 19 November 2020, https://about.fb.com/news/2020/11/bug-bounty-program-10th-anniversary/
[6] Facebook, *Vulnerability Disclosure Policy*, https://www.facebook.com/security/advisories/Vulnerability-Disclosure-Policy
[7] M Clark, 'Scraping by the Numbers', *Facebook Newsroom*, 19 May 2021, https://about.fb.com/news/2021/05/scraping-by-the-numbers/
[8] Other examples can be found at: https://about.fb.com/news/2020/06/automation-software-lawsuits/

Tools

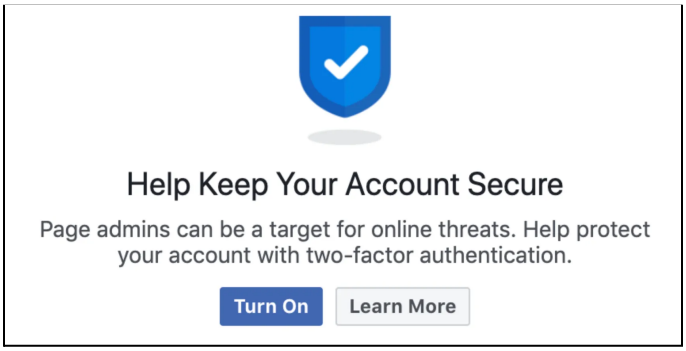
Users also play an important role in protecting themselves and their data. We make a number of tools available to support users to protect their cyber security. These include requiring strong and unique passwords, requiring secure browsing (HTTPS) that automatically encrypt a user's connection to Facebook, providing two-factor authentication, providing alerts for unrecognised logins and offering tips to recognise suspicious emails or attempts to steal a password or account information.

We've also built a dedicated hub for users outlining the steps we take to protect privacy and security and the tools they can use. It can be accessed at https://www.facebook.com/about/basics/stay-safe-and-secure

Proactive reminders

We regularly provide in-product reminders to prompt users to strengthen the security of their account by opting into two-factor authentication.

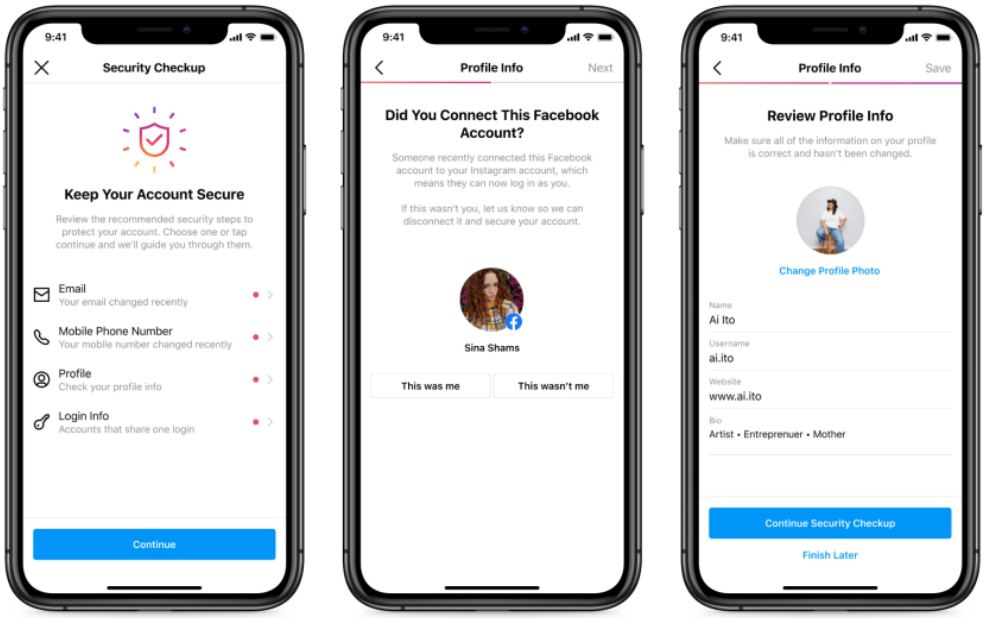
Facebook security prompt



Providing accessible information on how to keep your account secure

We offer easily accessible security tips for both Facebook[9] and Instagram[10], including an in product step-by-step guide to conduct a Security Checkup on your account. This feature, which was also recently extended to Instagram[11] guides users through setting up two factor authentication, checking login activity, confirming the accounts that share login information and updating account recovery.

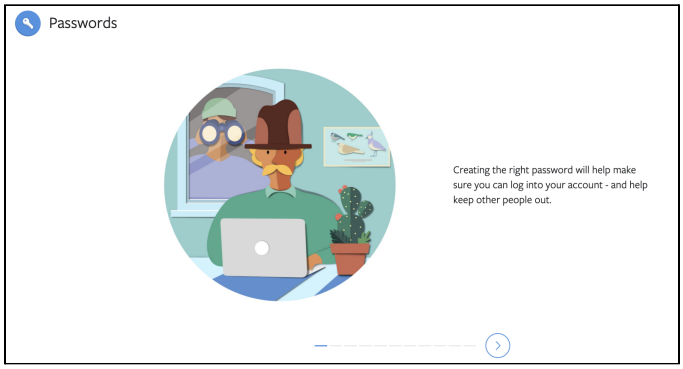
Instagram security checkup



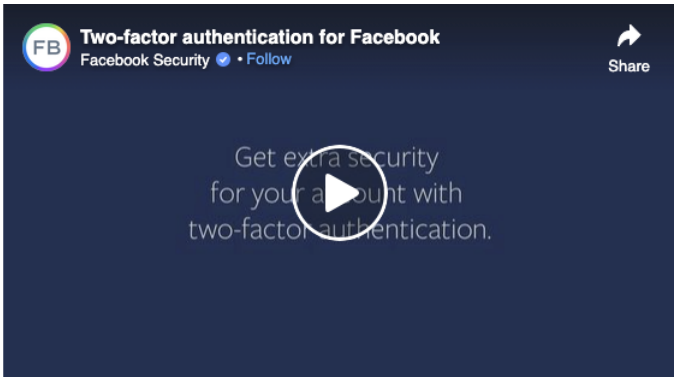
[9] Facebook, *Security Features and Tips*, https://www.facebook.com/about/security
[10] Facebook, Instagram Security Tips, *Instagram Help Centre,* https://help.instagram.com/369001149843369/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Privacy%2C%20Safety%20and%20Security&bc[2]=Login%20and%20Passwords
[11] Facebook, 'Keeping Instagram Safe and Secure', *Facebook Newsroom*, 13 July 2021, https://about.fb.com/news/2021/07/keeping-instagram-safe-and-secure/

We also provide tutorials on how to turn on each security control. Including:

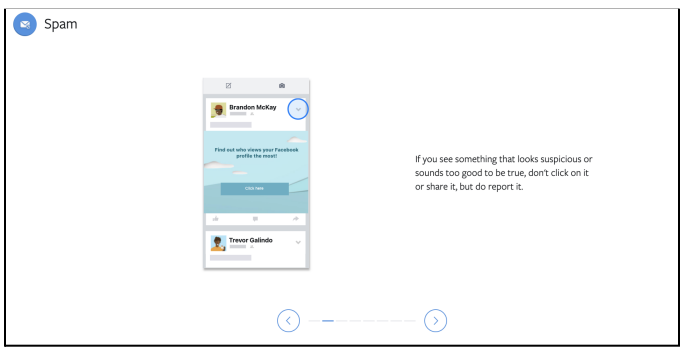
- A dedicated page to walk users through the process of choosing a strong and unique password.

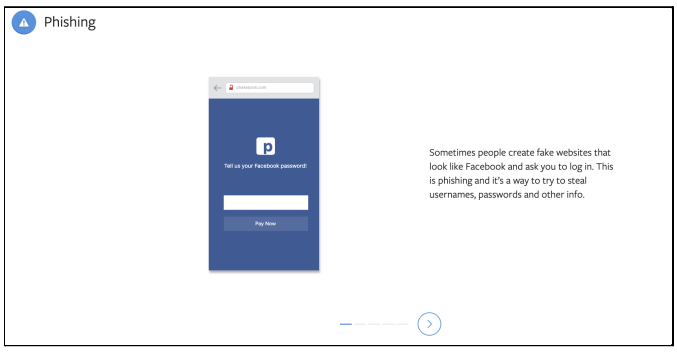


- Educational videos on how to set up and manage two-factor authentication to protect an account from improper access, and how to receive alerts about unrecognised logins.



- Providing tips on how to recognise spam and suspicious emails or messages.





Partnerships

We partner with industry, regulators and government to share our findings on threat actors, and raise awareness.

Partnerships to share intelligence

We know that threats and cyber espionage are rarely confined to one platform. We share our findings and threat indicators with industry peers so they too can detect and stop threat activity.

Each month we publish a list of threat activity that we have taken down. Through these reports we share identified malware hashes and malicious domains, as well as our findings on the latest tactics, techniques and procedures used by threat actors across the internet.[12]

We have also facilitated industry efforts to combat cyberthreats through threat signal sharing between industry peers through our ThreatExchange[13] API platform, which we launched in 2015. This program supports the sharing of threat information (e.g., malicious domains hosting malware, phishing scams, malware hashes) to help security professionals in participating organisations better tackle cyber threats by learning from each other's discoveries and making their own systems safer.

Partnerships to raise awareness

We raise awareness of cyber security issues through involvement in public campaigns, such as Scam Awareness Week, and providing helpful resources to increase awareness of cyber threats and prevent users from falling victim through scams, phishing or hacking.

We continue to be a partner for Scams Awareness Week, administered by the Australian Competition and Consumer Commission. In 2019 we produced an educational video to provide tips on how to spot and respond to scams online. The video was hosted by David Koch and received hundreds of thousands of views online[14].

[12] See for example: https://about.fb.com/news/2021/03/taking-action-against-hackers-in-china/; https://about.fb.com/news/2021/07/taking-action-against-hackers-in-iran/
[13] Facebook, 'Welcome to ThreatExchange', *Facebook for Developers Help Centre*, https://developers.facebook.com/docs/threat-exchange/getting-started/
[14] Facebook, *Tips with David Koch for 2019 Scam Awareness Week*, https://www.facebook.com/watch/?v=506418246798533

2019 Scams Awareness Week public service awareness campaign

Facebook has been working in a number of ways to support regional small businesses to develop digital skills. In 2018, we launched our Boost with Facebook program which is designed to support communities build local, small business resiliency and success. The workshop provides free digital skills education to empower small businesses with the tools they need to start and grow a business online at every stage of their journey. Since the launch of the Boost program, we are proud to say that Facebook has visited over 50 towns and cities and trained over 25,000 small businesses in Australia. These sessions often include support for small businesses to improve their cyber security, and we are considering opportunities to use our longstanding investment in Boost with Facebook to help support small and medium businesses to adopt better cyber security practices.

Overall comments

As well as the proactive work we undertake ourselves, we know that protecting cyber security requires a collaborative approach. Industry, governments, experts and the broader community all need to work together, as a weakness or vulnerability at any point can spread to other organisations.

We welcome this consultation process as an opportunity to discuss how the Australian Government and industry can collaborate to improve cyber security.

We welcome the chance to participate in a conversation about the right regulatory framework for cyber security issues. There are already some regulatory requirements in this space, such as the existing obligations under Australian Privacy Principle 11 in the Privacy Act. It is clearly important to ensure the community can have confidence that

their information will be protected with appropriate levels of security. Regulatory frameworks also require transparency to give the community confidence that we are making appropriate investments in protecting cyber security, and there are already reviews underway to assess if the existing regulation should be strengthened.

But there are also limits to regulation in relation to cyber security. These include:

- Adversaries change their tactics so quickly that prescriptive regulation will struggle to keep pace.
- Overregulation can encourage a mindset focussed on compliance rather than one focussed on continuous improvement and best practices.
- It is also important to make sure that regulation ultimately assigns penalties to bad actors who are perpetrating cyber security threats - not the companies that find themselves under attack.

It is also critical to ensure that regulation is targeted to address the areas of greatest risk. If the government is most concerned about small businesses or particular types of rogue actors (as outlined in the discussion paper), regulation will be most proportionate if it is tightly targeted at those areas of greatest risk.

Finally, we also recommend the Australian Government take a holistic and consistent approach to cyber security. Requirements around enabling law enforcement access to encrypted communications run the risk of undermining the cyber security benefits of encryption.

Response to specific proposals

Governance standards for large businesses

We acknowledge the discussion paper's perspective that it is important to ensure business governance structures give policymakers and the community confidence that cyber security risks are being appropriately handled.

To that end, we support the development of a draft set of voluntary governance standards for cyber security (described as option 1 in the paper), if they are developed in consultation with industry. Clear guidance and agreement on standards can provide greater transparency and confidence around companies' preparedness to deal with cyber security risks.

We recommend these standards should be voluntary, to help ensure they can adapt to changes in technology and the threat landscape and to best unlock industry collaboration with government. A principles-based set of expectations gives industry the greatest flexibility to determine how they should respond and, given the need for constant innovation in this space, flexibility is a great asset for adapting and keeping in front of threats from bad actors. We agree with the analysis in the discussion paper that a mandatory set of standards may be too onerous and costly.

A set of voluntary standards could use the Cyber Security Principles[15] already prepared by the Australian Cyber Security Centre as the basis for further collaboration with industry.

Minimum standards for personal information

It is clearly important to ensure the community can have confidence that their personal information will be protected with appropriate levels of security. We support the Government's intention to provide greater guidance for businesses about ways to manage personal information.

There are already some regulatory requirements in this space, such as the existing obligations under Australian Privacy Principle 11 in the Privacy Act. We suggest that the existing obligations remain reasonable and appropriate; however, there could be an opportunity to provide greater clarity and guidance (as intended by the Government) via the issuance of voluntary guidance on expectations by the Office of the Australian Information Commissioner. This could unlock the benefits of making expectations clearer.

A regulatory code registered under the Privacy Act risks duplication or inconsistency with the review of the Privacy Act that is currently underway by the Attorney-General's Department. This review specifically asked questions around the principle of user security and the outcome of the review is not yet known. It is difficult to comment on the potential benefits of a code without knowledge of the status of that review.

Stringent regulation is also not the best policy tool for changing consumer behaviour (as suggested in the consultation paper): the best method for encouraging better cyber hygiene by Australians is education and awareness. Mandating product changes (such as mandatory multi-factor authentication or pushing out patches at the direction of the company rather than the choice of the user), can present major technical challenges and

[15] Australian Cyber Security Centre, 'The Cyber Security Principles', *Australian Government Australian Signals Directorate*, https://www.cyber.gov.au/acsc/view-all-content/guidance/cyber-security-principles

practical difficulties in implementation. Mandatory product changes may also become quickly outdated.

Standards for smart devices

We support robust security features across a device's supply chain, and believe international standards have an important role to play in setting minimum expectations for cyber security for specific devices.

We support standards for smart devices, to the extent they are harmonised with international standards and provide voluntary options for businesses to adopt them in the first instance. Facebook is part of industry-leading and multi-stakeholder efforts to harmonise and standardise security best practices, for example, through the ioXt Alliance, the Global Standard for IoT Security.
The Australian voluntary code of practice for smart devices ("the Code of Practice: Securing the Internet of Things for Consumers") has not even been in operation for 12 months yet. It is too early to suggest that mandatory standards are necessary.

While we understand there have been a number of high-profile anecdotes about smart devices posing a vulnerability in an organisation's supply chain, it would be helpful to understand if the Department of Home Affairs holds data that suggests in aggregate smart devices hold a comparable or higher level of cyber security risk as relating to other devices and applications.

The discussion paper also explicitly seeks feedback on whether online marketplaces would be willing to voluntarily remove smart products that do not comply with a security standard. Facebook removes commercial content from our platform that does not comply with our Community Standards and we restrict access to content out of respect for local laws. However, we are not in a position to proactively search for and assess whether specific products comply with a particular standard. This obligation would pose an excessive regulatory burden.

Labelling for smart devices

We hold concerns about the discussion paper's proposals for a mandatory labelling scheme relating to cyber security of smart devices.

Firstly, it is not clear how the full suite of cyber security efforts undertaken by device manufacturers or operators can be reliably summed in a simple rating. As noted by the

Information Technology Industry Council (ITI) "no label can possibly cover all vectors of an attack, new vulnerabilities are continuously being identified, and labels are unlikely to cover the full range of security processes and activities manufacturers and end users must take to maintain security".[16]

Secondly, labels are not well-suited to the ever-changing and dynamic environment of cyber security. Technology and threats change regularly, and a smart device that may have had previously had a high level of security may be less effective in the face of new developments. "Expiry dates" also have flaws. The cyber security of smart devices is not static: software updates continue to maintain and improve the security of devices long after the initial point of purchase.

Thirdly, it is not clear that cyber security labels change consumer behaviour. Many of the international examples of international labelling schemes cited in the discussion paper are too new to assess their effectiveness.

Other jurisdictions such as Singapore have pursued a voluntary approach to smart device labelling. We suggest the Government waits until there is data on the effectiveness of schemes in other jurisdictions (like the Singapore scheme, the pilot in the US, or the new scheme in the UK), prior to proceeding with any labelling-specific regulation in Australia.

Responsible disclosure policies

As outlined earlier, Facebook may also occasionally find critical security bugs or vulnerabilities in third-party code or systems when we interact with them. In some instances, there may be significant complexity in working through how to resolve the bug with the partner. We have a Vulnerability Disclosure Policy[17] that sets out how we approach these situations. In general, we contact the responsible party as soon as reasonably possible, and we reserve the right to publicly disclose the vulnerability if we do not hear back within a reasonable amount of time. We prioritise the highest risk vulnerabilities. Our priority is to see these issues promptly fixed and that those impacted informed so that they can protect themselves by deploying a patch or updating their systems.

---

[16] Information Technology Industry Council, 'ITI Comments on Cybersecurity EO's Consumer Software Labeling Program', *Information Technology Industry Council,* 17 August 2021, https://www.itic.org/documents/cybersecurity/ITICommentsonSoftwareLabelingFinalVersion.pdf

[17] Facebook, *Vulnerability Disclosure Policy*, https://www.facebook.com/security/advisories/Vulnerability-Disclosure-Policy

We also welcome and reward those who raise bugs or vulnerabilities with our services via our sophisticated Bug Bounty Program, as outlined earlier.

Our experience has taught us that vulnerability disclosure can be very complex. There is no one-size-fits-all approach, as vulnerabilities can vary in terms of complexity and the best ways to communicate publicly about them.

For this reason, we caution against mandating prescriptive approaches to responsible disclosure. We encourage the Government to work with industry to see what can be achieved via voluntary uptake of responsible disclosure policies first.

We believe an industry-led renewed effort to encourage responsible disclosure policies would yield significant benefit. As an industry leader in this space, Facebook would welcome the opportunity to share more about our approach.

Health checks for small businesses

Given we would not be subject to the proposals relating to small businesses, we will leave comments on the specific proposals to small businesses themselves. As a principle, however, we strongly support the Government providing incentives and assistance for small businesses.

We also believe that larger companies like ours can have an important role to play in supporting small businesses. We outlined some of our existing work earlier in the submission, including our Boost with Facebook program which often includes support for small businesses to improve their cyber security.

Facebook is planning some additional work to support small businesses to enhance their cyber security, and we would be very happy to work with the Department of Home Affairs on how we can work together in this regard.

Legal remedies for consumers

Consumer law

The Discussion Paper seeks views on reforms to the Australian Consumer Law (ACL) and Privacy Act in relation to rights of recourse for cyber security.

There are already legal avenues available for consumers where a company is at fault for cyber security breaches. The ACL in particular already contains broad and flexible prohibitions designed to capture a wide range of conduct in trade or commerce. It also offers protections to consumers covering a wide variety of consumer products, including digital products.

The discussion paper presumes that current laws require strengthening, without any evidence presented to suggest that is the case. Just because the laws are untested does not mean they are deficient.

The ACL consumer guarantees are already being reviewed by Treasury at the request of Commonwealth, state and territory Ministers for consumer affairs. Any changes to consumer guarantees relating to cyber security need to be careful not to over-attribute responsibility to a company who is the victim of a cyber attack. A cyber security incident could occur for a multitude of reasons beyond the device or software supplier being at fault: it could involve user error, highly sophisticated malicious actors or some other factor beyond the control of the company.

Any proposed changes to the ACL should be reserved for the forthcoming consultation process being run by Treasury, rather than progressing separately through this process.

Privacy law

The paper also proposes a direct right of action through the Privacy Act. This proposal has been considered extensively, including via the Digital Platforms Inquiry and in the Attorney-General's Department's review of the Privacy Act which is currently underway.

We suggest any changes to the Privacy Act should be considered via the inquiry currently underway and led by the Attorney-General's Department, rather than via this process. This will help to ensure any privacy changes are aligned with the overall legislation.

Given the potential imposition on court resources, any direct right of action should only be contemplated for serious breaches that cannot be effectively addressed within the current dispute resolution framework under the Act. For that reason, we consider that any direct right of action should only be allowed where:

- the proceeding relates to a serious interference with privacy, and
- the Commissioner confirms that attempts at conciliation by the Commissioner have not been successful.

This would help to ensure that court proceedings are reserved only for the matters of most significance and which cannot be effectively dealt with through the existing regulatory framework. Our view is that the Commissioner remains best placed to deal with smaller matters in a way that is more cost and time effective for the consumer.

In addition, we note that a direct right of action might overlap with any new statutory tort for serious invasions of privacy. In our view, the creation of two new overlapping causes of action is unnecessary and may detract from the efficiency of the administration of justice. If a direct right of action is to be introduced, we suggest that it is drafted in such a way as to avoid overlap with any new statutory tort.