Australian Government

acma

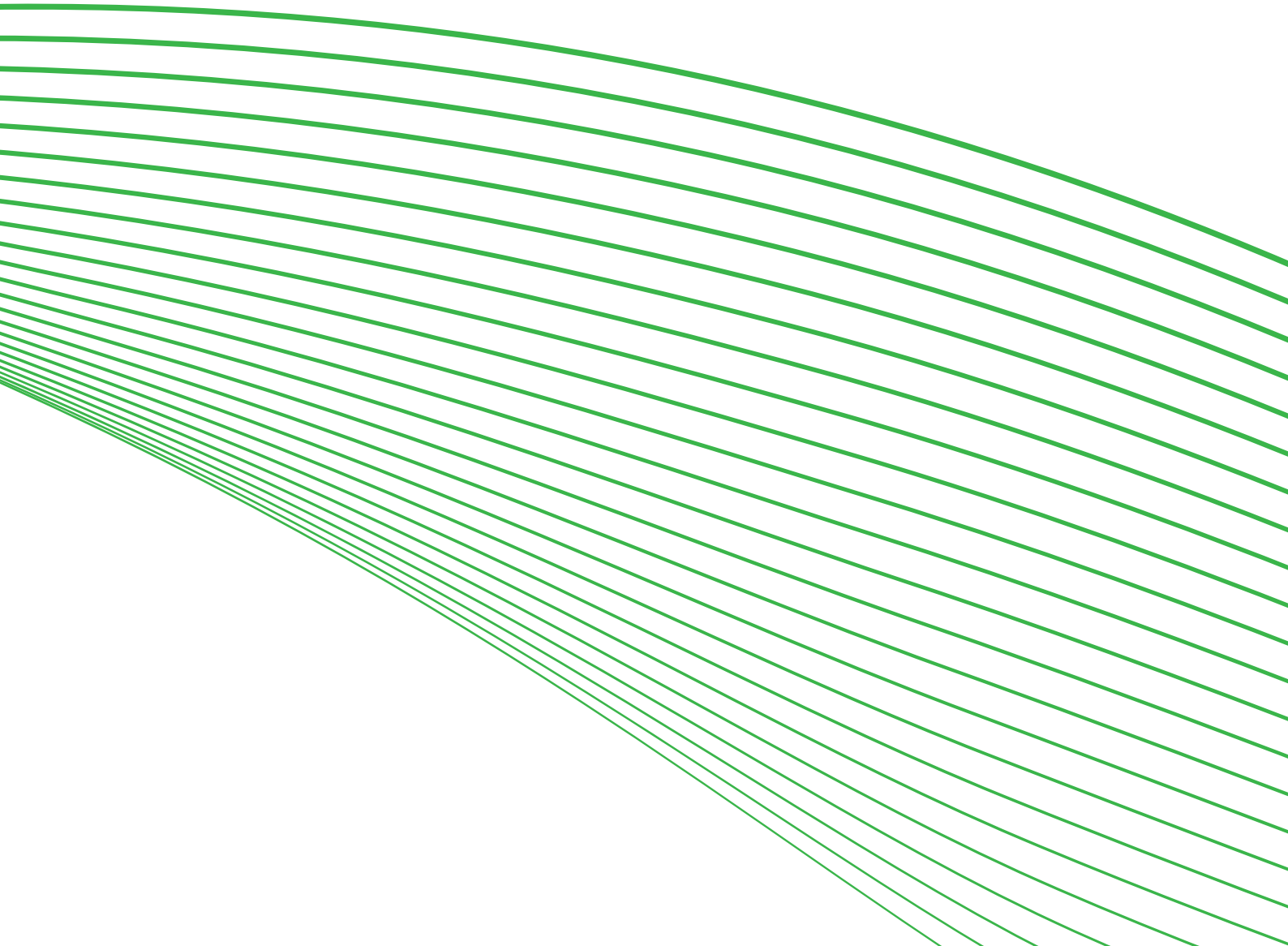
Australian Communications and Media Authority

researchacma

Cross-border regulatory strategies

Case studies in regulatory practice for a networked economy and society

OCTOBER 2013



Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

Published by the Australian Communications and Media Authority

Contents

Contents (Continued)

Executive summary

The global deployment of IP networks and the digitisation of content and communications have implications for the way that communications is regulated in Australia and internationally. Digitisation has created more complex, elongated and global supply chains that challenge traditional national approaches to regulation. At the same time, the open and participatory nature of the internet has allowed users to exercise greater control over aspects of their communications. As increasing amounts of both personal and institutional data is transferred internationally, regulatory approaches that are effective across jurisdictional boundaries are important in realising the social and economic benefits of a free flow of data across borders along with appropriate protections for the security of individuals and organisations.

research**acma**

This paper is part of the Australian Communications and Media Authority's (ACMA) research program, research**acma**, which is concerned with identifying communications and media matters of continuing significance to markets, society and government. This paper contributes to the ACMA's research theme on regulatory best practice and regulatory development, which examines the effectiveness of current regulation, identifies emerging issues that may require regulatory or non-regulatory solutions and where regulation may be updated and adapted to address contemporary communications and media issues.

About this paper

In its work identifying the enduring regulatory concepts that frame communications and media regulatory interventions, the ACMA noted common design features of converged regulation including flexible and calibrated regulatory tools, a recognition of shared responsibility between individuals, industry participants and government in an environment where individuals create as well as consume communications and media and the role of global engagement strategies.[1] This paper takes a closer look at the collaboration and engagement strategies used by regulators in Australia and internationally in response to the challenges presented by globalisation and the rise of participant users in internet-enabled communications and media.

A variety of tools and strategies has been used both domestically and internationally to deal with these issues, ranging from industry and citizen education to enforcement of compliance requirements. Increasingly, the cross-border nature of online activities requires that the regulatory tools in place at the national level be linked to multi-level, international regulatory strategies. While the discussion of tools is organised on the basis of international, national, industry and citizen/consumer tools, it is important to note that these elements may be connected to form an overarching strategy.

Three case studies illustrate different tools used to address these challenges:

- digital information management
- child sexual abuse material
- unsolicited communications.

[1] ACMA, *Enduring concepts—Communications and media in Australia*, November 2011.

The ACMA has a direct regulatory role under legislation in the cases of unsolicited communications, investigation powers in relation to online child sexual abuse material and the protection of personal data from public disclosure (data protection) aspects of digital information management. The digital transmission and consumption of copyright infringing content—another example of a digital information issue—is chosen for further examination because it offers insights into an area that has well-established international regulatory arrangements that are being tested by the impacts of communications and media technology changes and content innovation. The tools and strategies explored in each of the case studies illustrate the flexible approaches being employed to address different activities, concerns, and matters.

The environment

Globalisation and integration

The growth of the internet and associated changes in societal behaviour and business practices have altered the global market for content and communications. Global IP networks have also made it easier for supply chains to reach beyond national borders. Broadband network rollouts and technological innovations have encouraged the integration of formerly distinct industry sectors. In the communications and media sectors, content is now available over multiple distribution networks, including the internet and mobile networks.

Consumers are also interacting with these increasingly complex supply chains to source products and services from multiple entities. Data transfers were traditionally primarily business-to-business or government-to-government. Changes in technology and business practices have increased the scale of these transactions, and have fostered new business-to-consumer, government-to-consumer and consumer-to-consumer relationships.[2] Individuals transacting, searching for information and communicating online may routinely generate cross-border data flows.

New transactional relationships present several challenges to the effectiveness of traditional single jurisdiction and national regulatory approaches, such as determining the responsible party when consumers or citizens need to seek redress or assistance. Global supply chains may also hinder the delivery of domestic policy objectives. These are reliant on regulatory mechanisms designed for specific industry groups operating within a limited number of distribution channels. In addition, differences between national regulatory frameworks may place constraints on Australian market participants, limiting innovation and industry growth, and disadvantaging these firms when competing domestically and internationally. Furthermore, in defining the nature of the regulatory issue, social and cultural differences between nations could obstruct the implementation of an effective coordinated cross-border regulatory strategy.

Participatory users

Global access to, and adoption of, the internet has enabled individuals to play a greater role in areas that were previously the sole domain of industry suppliers or government. Broad access to IP networks has substantially reduced barriers to creating, transmitting and consuming data by ordinary citizens. The shift of services online—such as commerce, entertainment and communications—allows individuals to take a more active role in their consumption of services and their interactions with others, including organisations and government. For example, citizens are creating and distributing content and are expected to possess certain skill levels to be able to adequately participate in this digital environment.

[2] OECD, *The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines*, April 2011, p. 19.

The participation of citizens in a globalised digital economy presents challenges in establishing confidence in relevant regulatory rights and responsibilities.[3] For example, market participants who are not subject to Australian national legislation or industry codes of conduct may still be engaging with Australian consumers, businesses, and industry. Citizens may be adversely affected due to overlaps or gaps in the provision of protections and safeguards as a result. Equally, these new market participants may lack awareness of the rights and responsibilities of organisations in the Australian communications market, and may not be subject to the regulatory arrangements governing organisational behaviour.

Regulatory response strategies

New regulatory strategies continue to be developed to address these market-based, cultural and jurisdictional challenges. The strategies involve a greater focus on international cooperation and the shared responsibility of governments, industry and individuals for providing community safeguards and protecting the security of information and networks. Current regulatory tools incorporate a mix of initiatives, driven by international bodies, government, and industry. They aim to protect citizens and organisations, as well as encourage the commercial and social benefits emerging from global digital communications.

Analysis of the three case studies highlights four common design features of cross-border regulatory strategies:

1. harmonisation
2. collaboration
3. reliance on a mix of participants
4. use of broad-ranging tools.

These features facilitate a flexible approach to evolving regulatory challenges in a digital environment.

Harmonisation

A common design aspect in cross-border regulatory approaches is to use an international framework to influence and guide domestic regulatory responses. As national differences on these issues are inevitable, one response is to use an international framework as a regulatory design template, if possible. An example is the London Action Plan (LAP). Formed in 2004, this was the first international forum to address spam enforcement issues exclusively, and of which the ACMA is a signatory. The LAP outlines actions for public and private entities to cooperate on fighting international spam.

International frameworks allow varying levels of discretion in the implementation or design of national regulatory responses. Even with common regulatory designs, there will inevitably be differences between national legislative arrangements that can complicate cross-border regulatory responses. In these cases, proactive international engagement is an important tool to promote cooperation and encourage a productive outcome. The ACMA's ongoing dialogue with its international peers ensures that the Australian approach to unsolicited communications has been highly effective despite the differences in national legislative arrangements around the world.

[3] This refers to the need for confidence in policy settings and the clarity of the rights and responsibilities of regulators, industry and individuals as identified in the ACMA paper, *Enduring concepts—Communications and media in Australia*, November 2011, p. 17–18

Collaboration

Another common theme across the case studies is the emphasis on collaboration across borders. Global engagement has become a necessary strategic tool to identify emerging regulatory issues and to coordinate regulatory responses for electronic and internet-enabled communications.[4] There is a recognised need for sharing of experiences, expertise and information between participants, particularly for undertaking regulatory compliance and enforcement action.

Sharing knowledge and experience with other regulators, law enforcement and industry groups are necessary to build cooperative mechanisms and identify best practice approaches. There are a variety of ways regulators can do this internationally. Many regulators are members of international organisations, or signatories to cross-border agreements, that facilitate cooperation between countries. Examples include the Safe Harbor arrangements between the United States (US), European Union (EU) and Switzerland, that enables the free flow of data between those countries, and the Internet Hotline Providers' Association (INHOPE), which provides a forum for exchange of hotline management and operator expertise. The ACMA is a member of the Australasian Consumer Fraud Taskforce, which brings together government agencies in Australian and New Zealand that deal with the criminal aspects of spam, such as fraud and money-laundering.

Another aspect of collaboration is using purpose-specific databases to share information. Global IP networks represent an unprecedented opportunity for regulators to share information internationally and there is a proliferation of databases used for cross-border regulatory approaches. An example of a purpose-specific database is INTERPOL's International Child Sexual Exploitation Image Database.[5]

Reliance on a mix of participants

Complex supply chains, the integration of previously distinct industries and the increasing ability of citizens to participate using internet-enabled communications mean that a successful regulatory strategy is likely to have inputs and responsibilities for participants beyond the domestic regulator.

In a global digital economy, cooperation is required internationally as well as between government, industry and citizens domestically. For example, a common underlying principle of national hotlines designed to receive public complaints about child sexual abuse material on the internet is collaboration with law enforcement, education and industry bodies.[6]

Education programs directed towards citizens and industry are becoming a more prominent part of cross-border regulatory approaches. This recognises the more active role of citizens in the digital economy and the challenges of managing global issues through direct regulation. Examples include the ACMA's cybersafety program, Cybersmart, which includes information and strategies for individuals protecting their personal data in the online environment, and Google's 'Good to know' public campaign that provided information to consumers about privacy and data collection.[7] These programs assist in empowering citizens to protect themselves when interacting with content or communications originating both within and beyond national borders.

[4] Ibid, pp. 7–8.

[5] Refer to Appendix 3—Investigation of online child sexual abuse material case study for more information, p. 28.

[6] Ibid.

[7] See www.youtube.com, and refer to the privacy case study for more details.

Use of broad-ranging tools

In cross-border regulatory approaches, a range of tools are used to complement national legislation. Australia's approach to unsolicited communications is one example that relies on a range of interrelated tools—employing legislation, education programs for citizens and industry, and technology. When used in concert, these tools can be a powerful agent of change. This framework design has resulted in a reduction in the impact of unsolicited communications.[8]

In addition, a number of tools are being tested as new regulatory approaches develop in response to emerging issues. The digital information management case study is one such example. Four models for compliance and enforcement have emerged in respect to consumers' transmission and consumption of copyright infringing material. The models range from a broad taxation approach to enforcement of penalties against individuals infringing copyright.

Table 1 Case studies overview

Case study topic	Background	Reasons for selection
Digital information management	Digital information management is an increasingly important issue as citizens create, transmit and consume content over IP networks. Two aspects of digital information management are explored—the protection of personal data and copyright.	Digital information management issues highlight the evolution of regulatory arrangements in response to new challenges created by the digital economy.
Unsolicited communications	Digital technologies facilitate unsolicited communications across national borders. Cross-border regulatory approaches are integral to minimising the impact of unsolicited communications on citizens, as domestic legislation only addresses part of the problem.	This case study is an example of an effective multi-faceted cross-border regulatory approach deploying a combination of international, national, and industry-driven measures.
Online child sexual abuse material	The digitisation of content enables the trafficking of child sexual abuse material online across electronic communications networks. Protecting citizens from the production and distribution of child sexual abuse material requires international cooperation across sectors.	This case study highlights the increasing complexity of international supply chains, and the key role of communications regulatory strategies in an area that has traditionally been the sole domain of law enforcement agencies.

[8] See Appendix 2—Unsolicited communications case study.

Case study summaries

Digital information management

The concept of digital information management requires the treatment of data by network operators, service providers and other rights-holders to comply with consumers' preferences, relevant privacy legislation and community expectations. This case study analyses the regulatory and non-regulatory responses to cross-border challenges through the examples of data protection and consumers' transmitting and consuming copyright infringing material. Data protection is a complex concern in an environment where this information can be volunteered in a public forum, gathered to support the provision of goods and services, or potentially harvested without the individual's consent. The ability to take, reuse, combine and transmit data—including copyrighted content—over IP networks tests the concepts of intellectual property on which copyright is based.

Digital information management issues in the online environment highlight two sets of interests:

- the commercial, economic and social benefits that stem from the free flow of data
- the social interest and business benefits in protecting that data.

The regulatory arrangements governing the treatment of many digital information management issues reflect a mix of regulatory and non-regulatory strategies that respond to the changing environment in which data is distributed, communicated, stored or shared.

In addition to international privacy frameworks, individual governments have also worked together, participated in forums and collaborated on forming standards in terms of international approaches to data protection. Cross-border regulatory strategies for copyright are based on established international treaties or agreements.

To support these agreements, a mix of compliance and enforcement models are being used in combination with education and technological restrictions directed at individual content users and creators. There are four main models for compliance and enforcement of copyright provisions that are at varying stages of progress and levels of proven effectiveness:

1. graduated response models
2. industry or consumer levies
3. voluntary industry codes and compliance activities
4. identification models.

There is also a role for business and citizens in addressing digital information management issues. Industry codes, commercial agreements and technological applications are part of a range of industry responses. The role of the citizen is included in developing regulatory frameworks, reflecting the centrality of the concept of the digital citizen's rights and responsibilities in current regulatory approaches.

Unsolicited communications

Technological innovations in communications mean that there are now a range of ways to contact an individual, including via SMS, MMS, email, voice call (over public switched telephone network or IP), instant messaging and social networking sites. Unsolicited communications via any of these means can be from a domestic or international source, rendering domestic legislation less effective in isolation.

Consequently, cross-border unsolicited communications arrangements are marked by a multi-faceted approach of international cooperation, a legislative framework and industry and consumer education.

This case study is an example of an approach that has integrated objectives and strategies across international, government, industry and consumer-focused regulatory tools. For example, the Australian scheme for unsolicited communications combines a facilitative approach underpinned by compliance requirements. Education of industry and consumers is a priority and regulatory intervention occurs only when necessary.

Governments have introduced legislative frameworks domestically to combat spam and other unsolicited communications. Many countries have anti-spam legislation, as well as 'do not call' registers. Underpinning these legislative frameworks are education programs for industry and citizens. Industry education initiatives regarding the issue of unwanted telemarketing have been driven by industry associations, government and other stakeholders and form a key element of the regulator's work. Public education is also an important tool, in defining acceptable conduct parameters for industry, empowering consumers to engage with the regulator either by listing their phone numbers on the Do Not Call Register or reporting unwanted communications, and educating consumers on how to deal with issues such as identifying spam. One such education program is the FTC's 'Operation Spam Zombies,' an international campaign to educate internet service providers (ISPs) and other internet connectivity providers about hijacked or 'zombie' computers that spammers use to flood in-boxes internationally.[9]

The Australian Government employs a multi-faceted approach to combat unsolicited communications, incorporating industry and consumer education, a regulatory framework, and international cooperation. This approach has been the most effective path for dealing with unsolicited communications resulting in a reduction in the impact of unsolicited communications and changes to business practices and consumer behaviour.

Investigating online child sexual abuse material

IP networks enable wide distribution and simplify sharing of digitised content, including child sexual abuse material. Communications networks are consequently an integral part of the regulatory response to online child sexual abuse material, reflecting that cross-border regulatory strategies often require not only consistent legislative approaches, but also a wide range of technical expertise and other resources across the private and public sectors to be effective. The role of the communications regulator is key to this regulatory and enforcement process that have the dual objectives of protecting citizens and assisting law enforcement. For example, the ACMA is a member of INHOPE. The ACMA's participation in INHOPE includes exchanging information, contributing to policy development and best practice knowledge sharing.

Cross-border regulatory approaches use a combination of international covenants, international organisations—including alliances of law enforcement agencies, a network of internet hotlines, and other combinations of governmental and non-governmental agencies—and international research collaborations. For example, governments have enacted domestic legislation to address online child sexual abuse material. In addition, internet filtering is used by governments and industry as a mechanism with which child sexual abuse material can be restricted. Industry has developed codes of conduct and technological tools to allow individuals to restrict or block access to particular content (such as parental locks), and has formed partnerships across industry sectors and internationally to develop initiatives designed to stop child exploitation over the internet. Law enforcement officials also have a range

[9] FTC, *Partners Launch Campaign Against Spam 'Zombies',* press release, 24 May 2005.

of international technological tools, such as the Unlawful Images Automatic Search (also known as MARINA), that assist in gathering evidence in criminal cases and facilitates data exchange between national police forces.[10] Complementing these approaches are tools that enable citizens to protect themselves, primarily through education programs.

The cross-border regulatory approach to investigating and taking down online child sexual abuse material is an example of how the industries involved in the regulatory and enforcement process have had to expand in recognition of changing behaviours enabled by access to IP networks. For example, a substantial part of the total online trade in child abuse images has been commercially driven, used as a mechanism to harvest credit card and other personal information as part of organised criminal activity. Online payment operators, as well as credit card companies and other financial institutions, have engaged closely with law enforcement officials to combat this illicit online traffic.

[10] See Policing OnLine Information System website.

Findings

The similarities and differences between the three case studies highlight five key aspects of current cross-border regulatory arrangements:

1. the diversity of the approaches employed
2. the varied stages of progress in attaining goals
3. the importance of international cooperation
4. the rights and responsibilities of digital citizens
5. the complexity of regulating in a global digital economy.

Diverse approaches

Each of the approaches illustrated in this paper shows governments' attempts to balance the risks and benefits of intervention. For example, the social good in protecting citizens' personal data must be balanced against the social benefits of encouraging a free flow of data.

The case studies highlight the different approaches taken to achieve this balance, with varied levels of action and input by international organisations, governments, industry and citizens. Differences in approach can originate from the diverse objectives of these cross-border regulatory strategies and the type of regulatory problems addressed. For example, unsolicited communications regulatory approaches have been largely driven by national governments' legislative frameworks that are designed to protect their citizens from unwanted communications. In contrast, there are a variety of mechanisms that have been introduced to protect copyright introduced by government and industry.

Varied rates of progress

These three case studies show that cross-border regulatory approaches are at different stages of development in different industry sectors and regulatory activities. For example, data protection legislation is at various stages of review and development internationally. In addition to developing common standards and protections, part of this reassessment is looking at the role of the consumer within data protection cross-border regulatory approaches. In contrast, the unsolicited communications approach has well-defined roles for government, industry and consumers with common approaches by countries based on international frameworks.

In part, the varying stages of progress result from the amount of time the cross-border regulation approach has been in place and the complexity of the regulatory issues involved. Varied progress also reflects a changing environment in which regulatory approaches must be revisited periodically to ensure their continued effectiveness and relevance.

International cooperation

In all case studies, the regulatory strategies adopted have incorporated international cooperation, recognising the limits of unilateral action or national jurisdiction and the effectiveness of mutual understanding and cooperation. Any cross-border approach requires collaboration between regulators in different countries as they span different jurisdictional protocols, social and cultural environments, political expectations, and levels of capacity, technical expertise and resources.

A key element of each cross-border regulatory approach is some form of international cooperation. For example, there are three key international privacy frameworks—the

Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines, the EU Data Protection Directive and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. There are several international conventions providing a framework for addressing child sexual abuse material.

Ensuring effective cross-border regulatory approaches will involve finding tools to encourage commonalities across borders and incorporate the inevitable differences between countries.

Citizen empowerment

The rights and responsibilities of the digital citizen have a place in all of the cross-border regulatory strategies under examination. International practice suggests that recognising user empowerment is increasingly important in building an effective toolkit of regulatory responses. For example, the toolkits of the UK and Singapore regulators include powers relating to digital media literacy and cyber wellness respectively.

Digital citizens are envisioned as having both rights and responsibilities in these case studies. For example, citizens are recognised as having the right to be protected from unsolicited communications. At the same time, they have the responsibility to not access or share copyrighted content illegally, and can be prosecuted for doing so.

These case studies suggest that in some areas the role of a regulator can be a complementary and facilitative one—fostering digital media literacy strategies, focusing on empowering citizens to protect themselves and educating them on the tools to do so. One example is the ACMA's *Digital citizens guide*, which brings together a number of Australian Government and industry resources.

Complex environment

Globalisation and active citizens have created increasingly complex supply chains. This complexity means that the active involvement of a growing number of participants is needed for cross-border regulatory approaches to be effective. For example, the ACMA is a member of the Australasian Consumer Fraud Taskforce, a group of government agencies across Australia and New Zealand that, among other things, collaborate to deal with the criminal aspects of spam such as fraud and money laundering. Another example is the participation of the financial sector in disrupting the commercial distribution of child sexual abuse material.

Participants in the communications sector are also an important part of cross-border regulatory approaches. Digital information management cross-border strategies can involve third parties, such as ISPs or websites hosting content, in the enforcement process.

Global supply chains and the enhanced capacity of citizens to create and distribute content can result in complex cross-border regulatory problems that often require involving an expanded set of participants across industry sectors to contribute to market-based and regulatory solutions. These examples show that the communications and media sector is an integral part of an effective and relevant regulatory framework. The Australian government's cybersafety initiative is a multi-stranded regulatory approach comprising international cooperation, research, law enforcement, internet filtering and education. Participants include law enforcement, government, industry and the ACMA as well as international organisations and regulators. The ACMA's Cybersmart program is a key part of this initiative.

Appendix 1: Digital information management case study

Introduction

This case study explores the different government, industry and consumer-based tools used to address cross-border regulatory challenges generated by digital information management issues. The ACMA paper, *Enduring concepts—Communications and media in Australia*, identified digital information management as a concept of ongoing importance in media and communications. Digital information management covers the treatment of data by network operators, service providers and other rights-holders. Data can now be sent fairly easily from anyone with an internet connection to anyone else online and an increasing amount of data is stored within these IP networks. The definition of data incorporates a wide variety of services, functions and materials, including personal information, transactions, and content. The controls service providers put in place to protect and use this data is becoming an important issue. The concept of digital information management requires the treatment of data to comply with consumers' preferences, relevant privacy legislation and community expectations.[11]

Digital information management issues include the collection of information about individual online behaviour and copyright infringement. The popularity of online activities and services like social networking, search engines and e-commerce, coupled with new business practices, have raised transparency and informed consent concerns about the collection of personal data. One example of this is data collection by apps on smartphones and tablet devices. A study for the *Financial Times* found that many of the top fitness mobile applications transmit data to third parties.[12] Copyright protection is another dimension as the digitisation of content enables the easy transmission of content across borders, in both legal and illegal contexts. This case study uses the two examples of protecting data from unauthorised disclosure (data protection) and copyright to highlight the tools in place to respond to the cross-border regulatory issues posed by digital information management.

Copyright regulation is intended to promote the creation and distribution of content by protecting the ability of content rights-holders and producers to receive remuneration and recognition for their products.[13] It has a long history of working across international borders, as the content it protects is often widely distributed.[14] However, IP networks and technological innovations including the digitisation of content have irrevocably altered content production and distribution value chains. The ease of transfer of content across borders challenges the traditional copyright regulatory approach that assumes static business models centred on the physical publication of material. Citizens are now able to easily create, store, transmit and consume content over the internet. The major challenge is the greater ease of copying and distributing digital material outside established commercial arrangements in place for the supply and sale of content, and a variety of actions have been developed to respond to this issue.

Protecting citizens' personal data is increasingly challenging in this environment. Ease of data transfer has benefits for businesses and users but also increases the risk of

[11] ACMA, *Enduring concepts: Communications and media in Australia*, November 2011, page 7.

[12] Emily Steel and April Dembosky, 'Health apps run into privacy snags', *ft.com*, 1 September 2013.

[13] Barry Sookman, *A question of values* , 20 March 2012

[14] Copyright holders may hold copyright in foreign markets by virtue of the territorial protection of the respective countries.

data breaches to individuals and organisations.[15] It is difficult to quantify the magnitude of cross-border data flows and the extent of data breach issues occurring.[16] However, developments such as the widespread adoption of daily internet use, the growth in international internet traffic, take-up of internet-enabled devices (such as tablets and smartphones) and the rise of machine-to-machine communications, all suggest an environment of fluid data flows and cross-border data exchange.

These examples of digital information management issues highlight two sets of interests—the economic and social benefits that stem from the free flow of data, including across borders, and the social value and business benefits in protecting personal information. For example, individuals recognise the risks posed by the disclosure of personal data through common transactional and social interactions online. Australians disclose personal information online based on a risk-benefit analysis, weighing the perceived benefit (such as procuring a good or service) with potential risks, such as the risk of identity theft or damage to reputation.[17] In some circumstances, people are willing to disclose personal information when it benefits them, for instance for social networking or online shopping. Enterprises wishing to disclose customers' personal data for commercial purposes must balance the commercial benefits of this against the benefits of assuring customers and trading partners that their data will be secure.

The Australian context

The *Privacy Act 1988* (Privacy Act) forms the primary legislation governing privacy in Australia—including data protection—and sets requirements on private and public sector organisations for the collection, use and disclosure of personal information. The federal Office of the Australian Information Commissioner (OAIC) administers the Privacy Act. The Attorney-General's Department has primary policy responsibility for privacy issues related to personal information, including those issues raised by cross-border data flows. As part of this role, the department is engaged in developing international policy on cross-border disclosures, including the Trans Pacific Partnership Free Trade Agreement and in representing the government's views on these issues in a range of international forums, including the APEC Data Privacy Sub Group and the OECD Working Party on Information Security and Privacy. At the state level, there is legislation setting similar requirements on private sector organisations. There is also state legislation that sets requirements for the handling of health-related personal information.

In addition to the statutory frameworks for privacy and data protection, there are different common law actions that protect various privacy interests. These include breach of confidence, defamation and passing off. Although an action for invasion of privacy has been recognised by Australian trial courts, it has not been confirmed by appellate courts or the High Court. The Australian Law Reform Commission's (ALRC) 2008 comprehensive review of privacy recommended among 294 other things that a cause of action for serious invasions of privacy be introduced into Australian law. As part of the government's response to many of the other ALRC recommendations, the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 was introduced on 23 May 2012 and passed both houses on 29 November 2012. This Bill will make significant changes to the regulatory requirements for the cross-border disclosure of personal information. On 12 June 2013, the Attorney-General, Mark Dreyfus QC, asked the Australian Law Reform Commission to conduct an inquiry into the issue of

[15] OECD, *Report on the Cross-Border Enforcement of Privacy Laws*, 2006, p. 8.

[16] The OECD noted in 2006 in its *Report on the Cross-Border Enforcement of Privacy Laws* that ' … privacy and data protection authorities do not report receiving cross-border complaints in significant number ... Although this may indicate that there are not many privacy breaches with a cross-border dimension, it could just as well indicate that we lack information about this topic.', p. 8–9.

[17] ACMA, *Attitudes towards use of personal information online*, August 2009.

prevention of and remedies for serious invasions of privacy in the digital era. The ALRC will provide its final report to the Attorney-General by June 2014.

Australia's copyright regime is governed by the *Copyright Act 1968* and is under review. The ALRC has released an issues paper and a discussion paper, both entitled *Copyright and the digital economy*, as part of the inquiry into copyright legislation in Australia. The ALRC is due to report by 30 November 2013.

The role of the ACMA

As a communications regulator, the ACMA has multiple roles in digital information management issues and performs a number of regulatory and non-regulatory functions.

In data protection, the ACMA administers the *Telecommunications Act 1997* (the Telecommunications Act), which contains specific provisions relating to the protection of communications. This includes the disclosure provisions under Part 13 of the Telecommunications Act and privacy provisions in the Telecommunications Consumer Protection Code. The ACMA also administers more recent legislation such as the *Spam Act 2003* and the *Do Not Call Register Act 2006*, which are concerned with controls on unwanted communications. In addition, there are privacy provisions in various broadcasting industry codes of practice that are registered by the ACMA. The ACMA also delivers the Cybersmart program for children and young people, as well as general consumer information that include messages and practical advice about protecting personal data in the online environment.

The digitisation of content and services and the globalisation of the content market impact the ACMA's regulation of the communications market in Australia. Citizens are using communications networks to transmit and consume content. The globalised content market means that market participants who are not subject to, or not aware of, Australian national legislation or industry codes of conduct may still be engaging with Australian consumers, businesses, and industry. Consumers may be adversely affected due to overlapping or gaps in the provision of protections and safeguards as a result. At the same time, as active participants in the digital economy, consumers need to be aware of their rights and responsibilities in different contexts, including the creation, transmission and consumption of content.

International tools

International frameworks, agreements and other arrangements are an integral part of the regulatory response to cross-border digital information management issues and can influence domestic approaches to copyright and data protection issues. There are a number of highly influential international privacy frameworks in place, while copyright protection is managed internationally through a series of treaties and agreements.

International frameworks

Data protection is the subject of a variety of formal and informal international frameworks. The key international frameworks originate from the OECD, the EU, APEC and the Safe Harbor arrangements between the US, EU and Switzerland. Cooperation and collaboration between countries is a strong theme in these frameworks.

The OECD Privacy Guidelines, which encouraged adopting high-level principles and best practices for privacy protections have been in place since 1980. Newly revised guidelines were issued in 2013. The guidelines provide the foundation for developing national privacy laws in Australia as well as other nations. They also call for OECD member country cooperation through establishing procedures to facilitate mutual

assistance in procedural and investigative matters.[18] Building on this, in 2007 the OECD adopted a recommendation setting out a framework for cross-border cooperation in the enforcement of privacy laws, which included such measures as encouraging the sharing of information and fostering the establishment of an informal network of privacy authorities.[19] The most recent incarnation of the OECD Privacy Guidelines aims to improve cooperation between privacy authorities and the global interoperability of privacy frameworks.[20]

Harmonisation of treatment between countries is also an important objective of international frameworks. The European Commission (EC) has adopted proposals to amend the legislative frameworks for data protection, which have been in place since 1995 under the *Data Protection Directive.* The EC's proposals aim to harmonise the frameworks for data protection across different EU member states, as well as to apply data protection standards to countries beyond the EU's borders. The proposals aim to reinforce individuals' rights and help businesses, and several relate to cross-border data protection regulation issues, including:[21]

- People can refer data protection cases to the data protection authority in their country, even when their data is processed by an organisation based outside the EU.
- EU rules will apply even if personal data is processed abroad by companies that are active in the EU market.
- The use of streamlined procedures for 'adequacy decisions'. This is an acknowledgment that a given non-EU country ensures an adequate level of data protection through its domestic law or international commitments.

The EU parliament has not yet voted on the proposed legislative amendments to the *Data Protection Directive*.[22]

Unlike the adequacy approach taken by the EU, both the APEC Privacy Framework and the OECD principles are based on the concept of 'accountability'. In general terms, there are currently two internationally accepted approaches to dealing with cross-border data flows—the 'adequacy' approach contained in the EU Data Protective Directive, and the 'accountability' approach adopted by the APEC Privacy Framework in 2004. The adequacy approach places restrictions on the transfer of information to countries that do not have an adequate level of data protection standards. The accountability concept in the APEC Privacy Framework is derived from the accountability principle in the OECD Privacy Guidelines. The principle does not define accountability, simply stating that 'a data controller should be accountable for complying with measures which give effect to the principles' contained in the OECD guidelines.[23]

Other arrangements

Copyright is managed across international jurisdictions through a variety of international treaties and agreements that are generally relevant for the regulation of

[18] OECD, *Implementation of the 2007 Recommendation on Privacy Law Enforcement Co-operation*, 2010, as reprinted in Thirty Years After the OECD Privacy Guidelines, 2011, p. 76.
[19] OECD, *Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy,* 2007, p. 78.
[20] *The OECD Privacy Framework*, 2013.
[21] EC, 'Data protection reform: Frequently asked questions', 25 January 2012.
[22] John Burn-Murdoch, 'Europe deadlocked over data protection reform', *The Guardian*, 13 August 2013.
[23] OECD, *The OECD Privacy Framework,* 2013, p. 75.

online and physical copyright issues.[24] These have served to promote the development of international distribution channels and effectively supported rights holder's efforts in seeking remuneration and redress for their content.[25] One example is the two treaties instituted by the World Intellectual Property Organisation (WIPO)—the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty (commonly referred to as the WIPO Internet Treaties). The WIPO Copyright Treaty provides that copyright liability should not apply to a person or entity providing the physical facilities to communicate content.

There are also international agreements and arrangements designed to protect cross-border data flows. For example, the Safe Harbor framework, put in place in 2000, acts as a mechanism that enables the free flow of data between the EU and the US. Under the Safe Harbor arrangement, US companies can voluntarily adhere to a set of data protection principles recognised by the EU as providing adequate protection and thereby meet the requirements of the relevant EU directive. Since its inception, over 3000 companies have self-certified to the Safe Harbor framework.[26] The Asia Pacific Privacy Authorities (APPA) forum provides a means for privacy regulators in the Asia–Pacific region to form partnerships and exchange ideas about privacy regulation, new technologies and management of privacy enquiries and complaints.[27]

National tools

National tools used to respond to digital information management issues are varied. Tools include models for compliance and enforcement and establishing ways for national regulators to cooperate. National action on copyright issues has centred on implementing the provisions of various international agreements via enforcement and compliance regimes, albeit with slight differences in the interpretation of some definitions and policy objectives. For example, there are differences in what constitutes personal use, with some nations (such as Australia and Spain[28]) allowing the copying of legally purchased material to other formats for private use, while others do not (for example, the UK[29]). Another example is the differences in the length of copyright protection. In many nations the standard length of copyright for a book is 50 years after the death of the author, but in the US and some other nations it is 70 years.

Cooperation

It has been noted that to improve cross-border privacy enforcement cooperation, governments need to develop and maintain a number of domestic measures.[30] In 2007, the OECD set out a framework for cooperation in the enforcement of privacy laws. The 2013 revised OECD Privacy Guidelines reiterate the commitment by governments to enhance cooperation between privacy enforcement authorities. This

---

[24] International agreements include the Berne Convention for the Protection of Literary and Artistic Works 1886 (Berne Convention), the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention) and Convention for the Protection of Producers of Phonograms Against Unauthorised Duplication of their Phonograms (Geneva Phonograms Convention)

[25] Copyright Agency International, International copyright: treaties and organisations,10/02/2012.

[26] EU press release, 'EU-US joint statement on data protection by European Commission Vice-President Viviane Reding and US Secretary of Commerce John Bryson', 19 March 2012.

[27] OAIC, 'Asia Pacific Privacy Authorities'.

[28] Even then there are differences in what may be copied with Spain taking a broader view of what materials may be copied under private use provisions, and Australia limiting this to music.

[29] 'Unlike most countries, the U.K's current intellectual property regime makes it technically illegal to transfer content from CDs or DVDs on to a different format.' ComputerWeekly.com, *Government set to move UK copyright law into digital age*, 22/03/12.

[30] OECD, *Implementation of the 2007 Recommendation on Privacy Law Enforcement Co-operation*, 2010, as reprinted in compilation booklet *30 Years After the OECD Privacy Guidelines*, p. 74.

includes a commitment to improve information sharing to facilitate mutual assistance to one another in the enforcement of privacy laws.[31] The revised guidelines emphasise the importance of cross-border cooperation and that any restrictions to trans-border flows of personal data should be proportionate with the sensitivity of that data. Member countries are encouraged to support international arrangements which promote interoperability among privacy frameworks that are comparable with the OECD Privacy Guidelines.[32]

OECD member nations generally have national-level authorities responsible for enforcing data protection compliance, although in some countries (notably the US) this is part of consumer protection enforcement.[33] National regulatory bodies may exercise a variety of enforcement powers in relation to data protection. One important tool exercised by regulatory authorities is notification and information-sharing powers**.** For instance, in several OECD nations, regulatory authorities are able to notify authorities abroad of investigations that might concern them and whether they could share information with those authorities.[34] Effective cross-border data protection enforcement cooperation requires that regulatory authorities have sufficient authority to cooperate with international counterparts. For example, the APEC Cross-Border Privacy Enforcement Arrangement (CPEA) is a multilateral MOU arrangement that permits member regulators to exchange information, provide assistance and in appropriate cases allow for the transfer of privacy enforcement cases to a regulator in another jurisdiction.

Extra-territorial application for data protection

For some jurisdictions, national legislation for data protection is given extra-territorial application in certain circumstances. In Australia, as part of the reforms introduced by the Privacy Amendment (Enhancing Privacy Protection) Bill, the Government has adopted the accountability model developed by the OECD and more recently used within the APEC Privacy Principles. The new Australian Privacy Principle (APP) 8, which will apply to both private sector organisations and commonwealth agencies, adopts an 'accountability model' to ensure that information overseas is appropriately protected. An entity is permitted to make cross-border disclosures, having first taken reasonable steps to ensure the overseas recipient does not breach the APPs, but remains accountable for the acts and practices of the foreign recipient in relation to those disclosures. In general responsibility will only be transferred where the recipient of the personal information is subject to a law or binding scheme that protects the personal information in a way that is substantially similar to the protections afforded by the APPs, and there are mechanisms which an individual can access to take action to enforce that protection.

Compliance and enforcement models

The main compliance and enforcement models, in the context of consumers' transmitting and consuming copyright infringing material, are:

- Graduated response models—consumers receive warning notices and an escalating level of penalising actions.
- Industry/consumer levies—governments implement taxes and charges designed to reimburse content rights-holders.

[31] OECD, *Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data*, July 2013.

[32] OECD, *The OECD Privacy Framework,* 2013.

[33] OECD, *Report on the Cross-Border Enforcement of Privacy Laws*, 2006, p.12.

[34] Ibid, p. 22.

- Voluntary industry codes and compliance activities—governments actively promote industry based non-regulatory solutions such as codes of conduct, education programs and cross-industry agreements.[35]
- Identification models—in some jurisdictions, copyright holders are able to seek identification of infringers from ISPs enabling them to take further enforcement action against the individuals identified if they choose to.

The implementation of these models can be government or industry led.

Graduated response models

Graduated response models have a number of key commonalities aside from the escalation of warnings and enforcement actions:

- Implementation of the enforcement activities is generally the responsibility of ISPs. The various models differ in how or indeed if they are compensated for the increased administrative burden and associated costs.
- There is a growing trend to permit consumer redress. The US scheme includes appeals mechanisms, as does the UK scheme that is currently in development.

Graduated response models can be implemented at an industry or cross-industry level on a voluntary basis. US content rights-holders and ISPs have collaborated on such an approach. Under the new arrangements, ISPs will provide up to six warning/ educational notices to consumers who are accused of infringing copyrighted material via P2P file-sharing technologies. ISPs have a variety of mitigation options such as throttling a user's bandwidth speed or limiting access to the web. Accused individuals can request an independent review of their cases.[36]

Graduated response models are controversial and their effectiveness remains a matter for debate. One recent research paper commented on the present lack of evidence for a causal connection between the use of graduated response tools and reduced copyright infringement.[37] Many copyright owners have stated that piracy levels have fallen since the introduction of the graduated response model in New Zealand. However, the cost to issue notices through ISPs has been cited as an impediment to issuing infringement notices and consequently to effectively curbing piracy levels. There is a concern that piracy levels have plateaued, rather than continued to fall, as only a small number of infringement notices have been issued.[38] The French Government appears to regard HADOPI as a failure, with one of its ministers referring to the regime as 'unwieldy, uneconomic and ultimately ineffective'.[39] In 2013, the French Government replaced HADOPI with an automated fine system.

Industry/consumer levies

In a number of jurisdictions such as Spain and Canada, copying material for personal use is permissible and content rights-holders are reimbursed via industry levies or taxes on materials/services associated with copying material such as blank DVDs and CDs, burning software and digital media players. This model places greater administrative burdens on industry and government for the collecting and distributing the levy or tax. In addition, while this model addresses the issue of content producers receiving adequate remuneration and thus promoting creativity, it does not fully address the availability of illegally copied content.

---

[35] Discussed in the 'Industry tools' section of this report, p. 19.

[36] Rebecca Giblin, Evaluating Graduated Response, 14 September 2013, p.28–33.

[37] Rebecca Giblin, Evaluating Graduated Response, 14 September 2013, p.28–33.

[38] Tom Pullar-Strecker, 'Four in 10 Kiwis still flout piracy laws', Stuff.co.nz, 23 July 2012.

[39] Richard Chirgwin, 'France backs away from Hadopi,' *Theregister.co.uk*, 6 August 2012.

Identification models

In most jurisdictions, copyright holders who identify an IP address associated with copyright infringement can seek information about the subscriber from the subscriber's ISP. They can take legal action against the subscriber for copyright infringement. The process to do so is quicker and easier in some nations, such as Sweden, making it a more popular course of action in those jurisdictions. Arguably, the effectiveness of this system is primarily in the threat of action, rather than the action itself as copyright holders would need to consider the cost and benefits of prosecution. The Swedish branch of the International Federation of the Phonographic Industry has credited the scheme operating in that country, along with new music streaming services, for the reduction in file-sharing. It suggests that six out of 10 file sharers have either stopped or reduced their activities.[40] However, in the US where the system has been in place longer, copyright holders sought the introduction of more stringent graduated response models.[41]

Industry tools

Industry tools are a strong feature of digital information management responses. These tools include the production of an industry code, commercial agreements, and technological applications. For example, in the US, the overarching privacy framework proposed by the FTC and the Obama administration relies heavily on voluntary industry self-regulatory solutions as part of a multi-pronged strategy to provide privacy protection for consumers. A range of different industry self-regulation strategies have been put in place or proposed to address digital information management issues. In some cases, they are facilitated or encouraged by the government and form part of the overarching regulatory regime for data protection. In other cases, industry solutions may be independent from government strategies.

For consumers to make informed decisions about their online participation—particularly relating to the disclosure of their personal information—it is important that entities are transparent about their practices and policies relating to the use, disclosure and protection of that information. The Privacy Amendment Bill will require entities to have up-to-date privacy policies that include how information is used and the policies for protecting that data. The Bill will require entities to inform consumers about the likelihood of their information being sent overseas, and if practicable, where it may be sent.

Industry codes

Codes are a key mechanism for addressing data protection issues. In Australia, there are several industry codes of conduct that are designed to address online activity—a recent study found there are 16 codes of conduct, 13 that are active and three in draft form.[42] Some of these codes address the issue of data protection. For example, the Telecommunications Consumer Protection (TCP) Code incorporates disclosure provisions governing consumers' personal information. The TCP Code may apply beyond Australian borders as long as it involves a person/carrier/provider belonging to a section of the telecommunications industry under section 110 of the Telecommunications Act. The ACMA found that Telstra breached the TCP Code by making some personal customer information available via a link on the internet. The ACMA has issued Telstra with a direction to comply with the privacy clause in the

[40] Tim Cushing, 'Swedish Study Shows File Sharing And Music Buying Go Hand-In-Hand', *techdirt*, 18 March 2012.

[41] Greg Sandoval, 'RIAA chief: ISPs to start policing copyright by July 1', *c/net*, 16 March 2012.

[42] Chris Connolly and David Vaile, Cyberspace Law and Policy Centre, UNSW, *Drowning in Codes of Conduct: An analysis of codes of conduct applying to online activity in Australia*, March 2012.

code. The recently passed Privacy Amendment (Enhancing Privacy Protection) Bill will provide for an industry developed Credit Reporting Code of Conduct (the CR Code). The mandatory CR Code, will provide operational level guidance for implementing the credit reporting provisions in the Privacy Act. The CR Code is to be developed by industry and approved by the Privacy Commissioner.

The FTC's proposed privacy framework has a very strong focus on industry self-regulatory tools. The FTC's approach is to encourage companies to implement best practices to protect data, while also calling for the enactment of baseline legislation to protect consumers. A key self-regulatory measure that is part of the FTC framework is Do Not Track—a mechanism to allow consumers to control the collection and use of their online browsing data. While there are legislative proposals calling for the creation of Do Not Track, which, if enacted would mandate the FTC to establish standards for the Do Not Track regime, industry has already taken steps to develop Do Not Track tools. Browser vendors such as Mozilla, Microsoft and Apple have announced that the latest versions of their browsers permit consumers to instruct websites not to track their activities across websites. The Digital Advertising Alliance has developed an initiative that includes an icon embedded in behaviourally targeted ads. When consumers click on the icon, they can see information about how the ad was targeted and delivered to them, and they are given the opportunity to opt out of the advertising.

Enforcement via third parties

Content owners can seek to enforce their rights via ISPs. Implementation has been problematic with the recent Megaupload case in the US exemplifying the difficulty of ensuring compliance with the notices by the parties being asked to implement them.[43] In some jurisdictions, take-down notices are linked to safe harbour provisions. For example, the safe harbour provisions of the US *Digital Millennium Copyright Act* include responding to take-down notices as a condition of compliance. Like the graduated response models and identification models, this mechanism places increased financial and administrative burdens on third-party agents. Additionally, the evidentiary processes involved in identifying potential copyright infringing individuals are problematic. However, a 2009 UK study found 'that 70 per cent of file-swappers would stop sharing copyrighted files after a simple notice that their activity had been detected' suggesting that the notices can be an effective deterrent.[44]

Commercial agreements

There are a variety of agreements within and across industries that support content owner's rights. The most common are distribution agreements that seek to restrict access to content based on the consumer's geographic location. These require the content distribution channel to use filters such as the consumer's IP address, physical address or payment details to determine location and filter content for sale.[45] For example, iTunes has different virtual stores for different countries where content availability as well as the cost and release date in these stores differs. Although this process of limited availability allows Apple iTunes to negotiate separate agreements with national rights-holders, implementation can be problematic.[46] For example, in Germany negotiations between Google (for its YouTube platform) and GEMA, the German association that collects royalties on recorded media, broke down in 2009

[43] Chester Young, '$37 Million frozen in Megaupload case', *The Australian*, 24 January 2012.

[44] Nate Anderson, 'As Sweden's internet anonymity fades, traffic plunges', *Arstecnica,* 18 March 2012.

[45] Geo-blocking is being considered by the House of Representatives' Communication Committee Inquiry into IT pricing.

[46] Also called 'Windowing—refers to selling and reselling products over time using various distribution channels, for example, the film industry using cinemas, home video, rentals, cable, video-on-demand, free-to-air broadcasting', Ericsson, *ICT Policy for the Network Society,* p. 19

after the previous agreement expired.[47] Since then, all material controlled by GEMA has been unavailable on YouTube, and in 2010 GEMA sued Google over copyright infringement.[48] As a result, German consumers do not have access to a variety of music videos that are available in other jurisdictions.

Technological applications

There are a number of technological solutions that are used by content owners to restrict digitisation and online sharing of copyrighted material. An example of these applications is digital rights management (DRM). These can sometimes also be referred to as content rights management systems. DRM is a form of encryption usually found on physical copies of content and is aimed at preventing digitisation of the content and hence sharing of copyrighted material online. There are a number of different forms of DRM applications currently in use. While DRM prevents casual sharing of content, it has also given rise to applications designed to circumvent it. The *Copyright Act 1968* contains provisions against circumventing DRMs in Australia.

These applications restrict consumers' use of legally purchased content. These issues are yet to be fully explored and remain one of the discussion points of the growing digital economy.

Citizens

Citizens are increasingly disclosing personal information and accessing content via digital interactions. The shift of services online means that citizens are transmitting personal information to a range of organisations in varying contexts and sourcing their content from a range of suppliers.[49] Consequently, educating consumers on strategies to protect their own personal information and informing consumers about their responsibilities in terms of creating, transmitting and consuming content, are key parts of responses to the problems of personal data breaches and copyright infringement.

These strategies may be integrated into updated data protection frameworks that assume citizens must share responsibility for protecting their personal information. This reflects the changing role of the individual in cross-border data flows as changes in technology and business practices have fostered new business-to-consumer, government-to-consumer and consumer-to-consumer relationships.[50] Individuals transacting, searching for information and communicating online may routinely generate cross-border data flows. The role of the citizen has been recognised specifically in the EU's proposals for an updated data protection framework—in relation to the right to be forgotten—which has been framed as 'strengthening citizens' rights'.

Education programs and tools are available to assist citizens in protecting their personal data and informing them about copyright issues, such as the ACMA's Cybersmart program. The *Cybersmart Networking* online activity addresses the protection of personal data in the context of social networking and the website includes an information page for teenagers on P2P sharing. Industry-related or independent education programs are also available to consumers. Google's 'Good to Know' public campaign informs consumers about data collection and use, including using information to produce more relevant search results.

Another example is the online ratings tool Privacyscore. This tool scores websites and apps based on their data protection policies, with the aim of assisting internet users to

[47] GEMA—Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte.

[48] Kevin J. O'Brien, 'Google Ordered to Stop Copyright Violations on YouTube', *New York Times*, 24 April 2012.

[49] The rise of the participative citizen is explored in detail in 'The environment' section of this paper, p. 2.

[50] OECD, *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, April 2011, p. 19.

understand how websites handle and use the data collected by the site in the course of browsing, using third-party apps or other activities. It measures factors such as whether a website shares a user's personal data with other sites, how long a site retains that data and whether the site confirms that data has been released.[51] Such tools assist users to make more informed choices about the sites and applications they use. There are a variety of education programs and campaigns aimed at informing consumers about copyright issues. In terms of presentation and attitude the programs differ between organisations that are producing them but share common themes and messages. The main thrust of the material is on informing consumers that sharing copyrighted material is illegal and warning about the consequences. In addition, material highlighting the adverse impact of piracy on the content industry has also become more prominent in recent years.

Conclusion

There are multiple types of responses—incorporating government, industry and citizen action—to the challenges posed by digital information management. The regulatory arrangements governing the treatment of many digital information management issues reflect a mix of regulatory and non-regulatory strategies that respond to the changing environment in which data is distributed, communicated, stored or shared.

International cooperation and collaboration were strong themes in regulatory responses to cross-border digital information management challenges. International frameworks can be influential in the design of the domestic response and these frameworks can incorporate different approaches. The large volume of international data flows makes cross-border collaboration essential. Collaboration occurs in many contexts, both formal and informal, and includes the creation of agreements, such as the safe harbour provisions of the US *Digital Millennium Copyright Act*, and the formation of groups, such as the APPA, to enable cooperation in the exchange of experience and information.

Responses to the challenges posed by digital information management incorporate the role of the citizen. Consumer education, by regulators and industry, is an increasingly important part of data protection strategies. There is also a variety of education programs aimed at educating citizens about copyright issues.

[51] Tanzina Vega, 'A New Tool in Protecting Online Privacy', *New York Times*, 12 February 2012.

Appendix 2: Unsolicited communications case study

Introduction

This case study explores the regulatory and non-regulatory tools used to respond to cross-border challenges generated by unsolicited communications. Unsolicited communications can be described as a contact that was not sought or requested and has not been consented to previously. Technological innovation in communications has expanded unsolicited communications beyond telemarketing calls, faxes and email spam to incorporate mobile SMS and MMS and instant messaging. This case study will focus on the tools relating to unsolicited telemarketing and e-marketing (email) as the regulatory arrangements for these are more established.

Countries around the world have moved to address community concerns with the volume, inconvenience and intrusiveness of unsolicited communications. These unsolicited communications may be international or domestic in origin and consequently require a cross-border regulatory approach.

A variety of tools and strategies have been used domestically and internationally to deal with the problem, ranging from education and industry facilitation to enforcement responses in the form of financial penalties. A multi-faceted approach by the international community and national bodies has been the most effective path for dealing with unsolicited communications. The tools used by regulatory bodies, including consumer and industry education, have resulted in a reduction in the impact of unsolicited communications and changes to business practices and consumer behaviour.

The Australian context

The ACMA has responsibility for unsolicited communications, including telemarketing calls and spam in Australia, and uses a number of regulatory and non-regulatory tools to address them. Technological innovations have made geographic boundaries increasingly irrelevant and hindered the ACMA's ability to effectively independently apply Australia's regulatory arrangements. Effective regulation relies on effective multilateral cooperation. The ACMA has been proactive in sharing the Australian experiences with other countries advising on the development, implementation and enforcement of anti-spam legislation.

International engagement is a core part of the ACMA's response to spam, e-security, telemarketing and do not call issues. This engagement activity includes:

- information and intelligence sharing, which incorporates sharing of technical expertise, investigation and forensic skills
- learning and development, which incorporates developments in the global environment and keeping investigation expertise and techniques up-to-date. It also includes leveraging international engagement to achieve advancements at the global level in terms of managing or mitigating the effects of unsolicited communications in a way that benefits Australians.

Unsolicited telemarketing calls

In 2006, the Australian Government introduced the *Do Not Call Register Act 2006* (DNCR Act).[52] The DNCR Act established the Do Not Call Register, a secure database where citizens can list phone numbers to avoid receiving unsolicited telemarketing calls and marketing faxes, made from both within and outside of Australia. Businesses can check their call lists against the register in order to remove those numbers that are on the register. Under the DNCR Act, the ACMA is responsible for operating the register, handling consumer complaints, and promoting and facilitating industry compliance and enforcement. In addition, the ACMA enforces Australian industry standards for telemarketing, research calls and fax marketing.[53] These establish a minimum set of requirements for businesses making telemarketing calls or sending marketing faxes.

The Australian scheme is characterised by a facilitative role that promotes compliance. The scheme is supported with enforcement powers that may be used when required. It aims to educate businesses and citizens and to balance the need to protect citizens and allowing businesses the space to conduct their business. Regulatory intervention occurs only where necessary.

Spam

To respond to the economic and social impacts created by the proliferation of email-based spam, the Australian Government passed the *Spam Act 2003* (Spam Act) that prohibits the sending of unsolicited commercial electronic messages. The ACMA's role in regulating spam encompasses, among other things, compliance and enforcement of the Spam Act, educating businesses and citizens about spam, and initiating and cooperating internationally on anti-spam initiatives.

Australia's Spam Act was one of the first pieces of legislation against spam in the world. It takes an 'opt-in' approach to commercial electronic messaging, which requires recipient consent before commercial electronic messages can be sent.[54] This approach has influenced anti-spam legislation (and draft legislation) in a number of other countries, including Japan, Canada and Taiwan.

A reflection of the success of the Australian approach to fighting spam is the reduction in the percentage of spam passing through Australian networks. Australia was in the top 10 countries in terms of spam relayed through computer networks in the early 21st century. Australia had dropped to 52nd in the world for the period April–June 2012.[55] In the second half of 2012, the ACMA conducted research into consumer experiences with spam. Nearly half (47 per cent) of people who received spam emails in the previous month rated those emails as not particularly problematic, with perceptions of whether spam emails were problematic increasing with the number of spam emails received.

---

[52] The *Do Not Call Register Act 2006* (DNCR Act) and Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007 (the Industry Standard)—collectively referred to as the DNC legislation—set out the rules for telemarketers. The DNCR Act prohibits unsolicited telemarketing calls being made to numbers on the register. While the Industry Standard sets out minimum requirements for those making telemarketing or research calls. In 2010, legislative amendments expanded the program to include, among other things, unsolicited marketing faxes.

[53] Relevant standards are the Telemarketing and Research Calls Industry Standard 2007 and the Fax Marketing Industry Standard 2011.

[54] The ACMA participates in the Australasian Consumer Fraud Taskforce to cooperate with other government agencies that deal with the criminal aspects of spam, such as fraud and money-laundering.

[55] Sophos Labs research quoted in the ACMA report, *The ACMA—meeting our standard: To be, and to be recognised as, the world's best converged communications regulator*, March 2013, p. 59.

International tools

Many countries have recognised that without international cooperation, their domestic anti-spam legislation is insufficient. This has led to broad use of the OECD's Anti-Spam Toolkit, a package of recommended policies and measures aimed at assisting industry and governments to work together to combat spam. The toolkit provides guidance on regulation, enforcement, industry involvement, technical solutions and education and awareness programs, allowing policy makers, regulators and industry to structure their regulatory frameworks in a consistent way.

Australia has made international cooperation a key element in a multi-tiered strategy to combat spam. Australia supports and participates in cooperative arrangements between countries that involve working collaboratively to deal with spammers beyond national borders.[56]

The ACMA has been recognised for its international efforts in the fight against spam. In 2009, the ACMA received a nomination for a United Nations Public Service Award for its work in the international spam community, particularly through participation in the London Action Plan (LAP).

International agreements

With other countries, the ACMA participates in a number of multilateral and bilateral agreements that target unsolicited communications. For example, the LAP's focus is spam and members include regulators, law enforcement and industry. The LAP assists regulators and other parties in establishing contacts that are essential for international cooperation and collaboration in the fight against spam. The ACMA also participates in the International Do Not Call Network, which has members from 15 countries. The network was created to enable international cooperation on enforcement and education activities and to work with industry to find technology solutions to ensure do not call regimes retain their efficacy.

International cooperation

Regulators share information and tools with one another to assist in responding to spam. For example, the ACMA, Canadian Radio-television and Telecommunications Commission (CRTC) and the US Federal Trade Commission collaborated to share intelligence on a phone scam in which parties, masquerading as representatives of Microsoft, appeared to make telemarketing calls to citizens. This resulted in court orders freezing the US-based assets and accounts of parties alleged to be linked to these scams. The ACMA also shares spam analysis software under a free licence with the CRTC, the Dutch Authority for Consumers and Markets, and the New Zealand Department of Internal Affairs.

Cyber security programs can also address spam issues by going to their source, for example, by identifying botnets producing spam.[57] Much international liaison and cooperation on botnet matters is with non-government organisations, such as Shadowserver, Team Cymru, anti-malware companies and the international CERT community.

In 2007, after close collaboration with the ACMA, the ITU produced a draft botnet mitigation toolkit that was 'inspired by' the ACMA's Australian Internet Security

[56] Meyer Potashman, *International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society*, 29 B.C. Int'l & Comp. L. Rev. 323 (2006).

[57] An example is the icode, a voluntary code of practice for Australian ISPs that has four main elements—a notification/management system for compromised computers, a standardised information resource for end users, a comprehensive resource for ISPs to access the latest threat information, and a reporting mechanism in case of extreme threat back to CERT Australia.

Initiative (AISI). The AISI program provides daily reports of malware infections to participating Australian internet providers identifying current malware infections resident on their networks. These providers—who cover more than 95 per cent of Australian residential internet users—are expected to use the information provided through the AISI to identify, on their networks, internet users whose computers are infected, inform those users about the infection and provide them with assistance to remove it.

Cross-border engagements on cybersecurity issues are often undertaken through trusted informal networks, generally to expedite the action being taken. One example is the international response to phishing emails sent in 2012, which were purported to have come from the ACMA. The ACMA succeeded in having the fake web pages that the emails linked to rapidly remediated through utilisation of these networks.

National tools

Legislative frameworks

Many countries have seen deterrent value in a legislative approach. For example, Australia and EU member states have passed legislation to regulate unwanted telemarketing and spam. Both Australia's Spam and Do Not Call Acts provide a range of enforcement options, including formal warnings, enforceable undertakings, infringement notices, and action in the Federal Court for the recovery of penalties payable for contraventions of civil penalty provisions. These are designed to ensure compliance and to deter unlawful activities relating to unsolicited communications. The EU has directed its member states to implement a series of coordinated measures to target spam including effective enforcement of laws and strategies to ensure communications between the various regulatory agencies. Article 13 of the European Union Directive on privacy and electronic communications (2002/58/EC) provides that member states shall take appropriate measures to ensure that unsolicited communications for the purposes of direct marketing are not allowed without the consent of the subscribers concerned (opt in) or in respect of subscribers who do not wish to receive these communications (opt out), the choice between these options to be determined by national legislation.

Do not call registers

Do not call registers operate in a number of countries and use a variety of approaches. The Australian Do Not Call Register allows citizens to assert their right not to be contacted by telemarketers and encourages and enables industry compliance, supported by a graduated compliance model.

Similarly, the CRTC is responsible for investigating whether a telemarketer made a telemarketing call to a number on its do not call register. Both the ACMA and the CRTC outsources initial complaint-handling to a register operator, who will make an initial assessment as to whether legislation has been contravened and refer the matter to the regulator.

In contrast to Australia and Canada, the approach to unsolicited telemarketing calls in the UK involves a co-regulatory regime administered by the Telephone Preference Service (TPS) and enabled by the Privacy and Electronic (EC Directive) Regulations 2003. The TPS is administered by the direct marketing industry, while investigations are conducted by the Information Commissioner's Office as part of the UK Government.

Alert programs

The ACMA provides automated reports identifying suspected phishing web pages to all the major Australian financial institutions, the Australian Taxation Office and some other commercial organisations routinely subjected to phishing campaigns. Phishing is

defined by the anti-phishing working group (APWG)—a worldwide coalition comprised of representatives from governments, global Internet governance bodies and commercial entities—as ' … a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials'. The ACMA's automated phishing reports are mainly derived from spam reports provided to its Spam Intelligence Database. Over 33,000 automated reports were provided to stakeholders in the 2012–13 financial year.

Industry tools

Industry education programs

Education of industry participants is a vital part of the unsolicited communications regulatory approach, as the effectiveness of the legislative framework depends on compliance by industry. Industry education initiatives on the issue of unwanted telemarketing have been driven by industry associations, government and other stakeholders and form a key element of the work of the regulator. For example, in telemarketing, the Association for Data-driven Marketing and Advertising (ADMA), produces publications to assist industry with compliance and best practice, and runs compliance courses for businesses.

The ACMA has a role in assisting marketers to understand their legislative obligations in e-marketing and telemarketing. This educative role is a key pillar of the ACMA's compliance approach. The ACMA provides information that helps the marketer to identify how a call was made or fax was sent to a number on the register, as well as equipping it with practical guidance on how to achieve best practice compliance. The ACMA produces two blogs—Successful e-marketing ... it's about reputation and Better telemarketing … take the right line—aimed directly at businesses that engage in telemarketing, fax marketing and e-marketing. The blogs promote and encourage businesses to comply with the rules and encourage best practice, highlighting how compliance with the Spam and DNCR Acts can enhance a business's reputation. The ACMA, in concert with industry, developed the *Do Not Call Register Act 2006—Compliance guide,* which contains detailed guidance on measures marketers can take to comply with the DNCR legislation.

Citizens

Public education is an important tool in defining the parameters of acceptable conduct for industry. Telemarketing and spam education requires a collaborative approach between the ACMA and industry bodies, consumer groups and other government agencies to fully engage with the Australian public. To facilitate this objective, the ACMA has developed an educational approach with key strategies for citizens including:

- promoting awareness of the need to identify, respond and protect themselves from unwanted communications
- increasing awareness and understanding of the rules around unsolicited communications
- assisting them to more effectively engage with the ACMA on complaints, reports and enquiries about unsolicited communications.

The ACMA regularly publishes telemarketing and spam scam and phishing alerts on its website and engages with members of the public on telemarketing and spam-related issues via Facebook and Twitter. It uses these channels to issue alerts and warnings about phone, email and SMS scams in circulation. The ACMA has also established links to its e-marketing and telemarketing education information externally via a variety of other Australian and state government agencies and departments, such as the Australian Consumer and Competition Commission and the Australian Information Commissioner.

Conclusion

The tools used to respond to cross-border unsolicited communications challenges are an example of an effective multi-faceted cross-border regulatory approach. International, national, and industry-driven measures are used in concert to reduce the level of unsolicited communications experienced by citizens.

Formal and informal cooperation and collaboration between regulators, including participation in international forums, are integral to dealing with cross-border unsolicited communications issues.

There is also a strong emphasis on education, geared towards both industry and citizens. In addition, national frameworks for unsolicited communications, such as do not call registers, empower citizens to protect themselves.

Appendix 3: Investigation of online child sexual abuse material case study

Introduction

This case study explores the regulatory and non-regulatory tools used to respond to cross-border online child sexual abuse material issues. The digitisation of content and widespread deployment of IP networks enable broad distribution and sharing of digitised content, including child sexual abuse material. The use of communications networks in the distribution and sharing of child sexual abuse material online means that communications regulators have a key role to play in assisting the regulatory and enforcement process designed to combat the proliferation of this content.

The international arrangements for dealing with online child sexual abuse material is an example of the emerging role of the communications regulator as a key participant in processes designed to support law enforcement agencies in combating this material while offering appropriate safeguards for citizens. The multi-faceted arrangements designed to combat the production and distribution of this material involves both international and domestic law, industry agreements and actions by individuals.

The Australian context

The ACMA is responsible for administering the regime for online content in Australia. Online content is regulated under the Online Content Co-Regulatory Scheme (the Scheme) established under Schedule 5 and Schedule 7 of the *Broadcasting Services Act 1992* (BSA). The Scheme aims to address community concerns about prohibited content found online and acknowledges that government, industry and the community all have roles to play in the effective co-management of online safety issues. Due to the proliferation of content hosted overseas, the regulatory framework enables cross-border mechanisms (with law enforcement endorsement).

The BSA recognises that prohibited content hosted outside Australia cannot be promptly dealt with through take-down notices or law enforcement action. It provides for flexibility of alternative procedures to deal with material that would be the subject of law enforcement notification and a take-down notice if it was hosted in Australia, and allows the industry to develop effective arrangements that are technically and commercially feasible. When prohibited or potentially prohibited content is found to be hosted overseas, the ACMA refers the specific web address that of the content to Internet Industry Association accredited Family Friendly Filters. This action is in accordance with the BSA and registered Internet Industry Codes of Practice. Under the codes, ISPs are required to provide approved filters to their subscribers at or below cost price.

There are two approaches to dealing with child sexual abuse material. If the content is hosted domestically, the ACMA refers the matter to law enforcement agencies and then issues a take-down notice. If the child sexual abuse material is hosted overseas, it is referred to INHOPE—the International Association of Internet Hotlines—for referral to law enforcement agencies in the host country, if appropriate, or to the Australian Federal Police (AFP) for action through Interpol. INHOPE effectively acts as a 'fast lane' for reporting child sexual abuse material across international borders. Notifications through INHOPE effect rapid law enforcement action and take-down in the country where the content is hosted, while preserving the legal sovereignty of the countries involved. The ACMA is a member of INHOPE and engages with the network

by exchanging reports of overseas-hosted child sexual abuse material to the country in which the content is hosted or appears to have been produced in, receiving and actioning reports from other member countries, contributing to policy development and best practice knowledge-sharing.

Significantly, INHOPE is an active member of such initiatives as the European Financial Coalition against Commercial Sexual Exploitation of Children Online.

International tools

International conventions and organisations

International conventions provide a framework for addressing online child sexual abuse material globally. Signatories are required or encouraged to implement arrangements domestically. Key international covenants are the Convention on the Rights of the Child and its Optional Protocol, the Council of Europe Convention on Cybercrime, and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. The EC has coordinated and supported various efforts to combat illegal content through a Safer Internet Program. The program co-funds a variety of educational and research projects as well as initiatives to set-up illegal content reporting hotlines.

International organisations are another important tool for facilitating cooperation across borders on the issue of child sexual abuse material. Collaboration across jurisdictions and with industry (such as ISPs providing police with IP addresses) is critical in supporting the role of law enforcement. There are several international organisations that specifically facilitate law enforcement collaboration, including:

- Virtual Global Taskforce—an international alliance of law enforcement agencies. It aims to build an effective international partnership to protect children from online child abuse.
- INTERPOL—a central global point of contact for police, INTERPOL enables investigations at the local, national and international levels and coordinates large-scale investigations involving multiple member countries.
- INHOPE—coordinates a network of internet hotlines across the world and supports those hotlines in responding to reports of online child abuse. INHOPE places a strong emphasis on collaboration, requiring members to have working relationships with relevant law enforcement, education and industry bodies.
- Global Cyber Security Agenda Child Online Protection Initiative (COP)—the COP brings together a broad spectrum of governmental and inter-governmental agencies, law enforcement agencies, industry and civil society representatives to form a collaborative network that shares knowledge and experience and develop tools to protect children online.

Technological tools and databases

Law enforcement officials use a number of international tools that help gather evidence in criminal cases and facilitate data exchange between national police forces to combat the production and distribution of child sexual abuse material. These tools range from technological tools, like the unlawful images automatic search that scans suspect computers for files related to child abuse images, to databases that can be used to share data, such as INTERPOL's International Child Sexual Exploitation Image Database, to international networks that work together to share experience and knowledge, such as CEOP's International Child Protection Network. INHOPE has released an integrated reporting system that allows individual hotlines to upload information on reports to a central database. A shared database encourages greater efficiencies by identifying where the same images are being investigated by multiple parties. Another tool is Microsoft's PhotoDNA technology that aids in finding and

removing child sexual abuse material. Services including Bing, SkyDrive, Hotmail and Facebook use PhotoDNA technology.

National tools

Legislation to address online child sexual abuse material

Several jurisdictions—including EU member states, the US, Japan, Canada and Australia—have put in place national laws to address online child sexual abuse material. While the legislative scope and approach varies between countries, there is a relatively high level of agreement as to what constitutes child sexual abuse material. This provides a good foundation for international cooperation. In November 2011, the EU adopted the Directive of the European Parliament and the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material. Among other actions, the directive criminalises forms of child sexual abuse and exploitation not currently covered by EU legislation, such as:

- grooming, online pornographic performances and viewing child sexual abuse material without downloading files
- establishing lower thresholds for applying maximum penalties
- ensuring that offenders who are EU nationals face prosecution for crimes committed outside the EU
- providing child victims of the offences covered with assistance, support and protection, including for claiming compensation
- sharing data relating to the criminal convictions of sex offenders between relevant authorities in member states
- introducing mandated removal and optional blocking of websites containing child sexual abuse material.

Japan has passed a series of laws to protect children in cyberspace. The Act on Punishment of Activities Relating to Child Prostitution and Pornography and the Protection of Children is designed to reduce the prevalence of child sexual abuse material and child prostitution and to protect children from sexual exploitation and abuse. In addition to these laws, the cabinet office together with nine ministries and agencies, including the National Police Agency and the Internet Affairs and Communications Ministry, introduced general measures to eliminate child sexual abuse material and establish a council with representation from the private sector and civil society organisations to raise public awareness.

New Zealand is less structured in its treatment of child sexual abuse material. Legislation defines objectionable content, which includes child sexual abuse material, and such content can be investigated by the Department of Internal Affairs. However, unlike in Australia, there is no clear mechanism under which the government can issue a take-down notice. The New Zealand system relies instead on a classification system and there is no direct online regulation of content. In July 2009, the New Zealand Government's Department of Internal Affairs announced that it would be introducing software for voluntary use by ISPs that would form the basis of 'The Digital Child Exploitation Filtering System.'

Hotlines

National hotlines enabling reporting of child sexual abuse material have been established around the world and complement existing law enforcement activity. INHOPE coordinates a network of 43 hotlines in 37 countries covering a large proportion of the world's population. These hotlines can be industry, NGO or government operated.

Industry tools

A number of industries can have a key role in policing child sexual abuse material, through codes of conduct, membership of industry bodies, and the provision of filtered software. For example, industry codes are part of the regulatory framework in Australia, setting out a range of obligations on ISPs to provide their customers with tools and information to assist them to use the internet safely. To comply with registered Internet Industry Codes of Practice, ISPs are required to make optional end-user (PC-based) filter software available at or below cost price to their subscribers. The filter products have been tested and accredited by the Internet Industry Association as meeting certain requirements and at a minimum receiving updated lists of URLs of prohibited and illegal content from the ACMA.

Industry bodies

Industry bodies, collaborating with members from government, law enforcement and industry, can play a key role in policing child sexual abuse material. For example, the UK Internet Watch Foundation (IWF), a charity largely funded by the internet industry, plays a key role in development of regulatory tools to deal with online child sexual abuse material in that country. The IWF is a not-for-profit organisation that runs in collaboration with government, industry, the police and the public. It has acted as a hotline and has worked in conjunction with the police, the Home Office and the Crown Prosecution Service to receive public complaints and determine whether particular web pages contain child sexual abuse material. Another example is Canada's Cybertip, which is run by a charitable organisation. The Canadian hotline maintains a list of URLs hosted outside of the country containing child sexual abuse material and distributes this to ISPs. Eight major ISPs in Canada voluntarily block the Cybertip.ca list, providing coverage to almost 90 per cent of Canadian internet subscribers.

Organisations involved in the communications and media sector have also contributed to the policing of child sexual abuse material. Microsoft has partnerships with law enforcement agencies and ISPs in 15 countries to develop initiatives designed to stop child exploitation over the internet. An example of this occurred in Australia when Microsoft helped provide law enforcement with information to assist Operation Auxin, which ultimately led to 150 people being charged with more than 2,000 offences. The Child Exploitation Linkage Tracking System is a software system developed by Microsoft Canada that allows police services to communicate information that previously could not be shared, overcoming the technical boundaries that prevented effective coordination among police services in the past.

Internet filtering in cooperation with government

In a number of countries, including Australia, the UK, and a number of European countries, industry has taken steps to block content identified as child sexual abuse material where it has not been possible to promptly take down the material in the country where it is hosted. In Australia, some ISPs are blocking domain names on request from the AFP, using information supplied by Interpol. British Telecom, the UK's largest ISP, administers the Cleanfeed program that filters content deemed inappropriate by its inclusion on a list of websites compiled by the IWF and is oriented towards filtering images of child abuse. ISPs, mobile network operators, content providers and search engines such as Google and Yahoo are provided with a copy of the list and are encouraged to remove access to websites listed on it.

Financial institutions

A substantial part of the total online trade in child sexual abuse material has been commercially driven. Organised criminals have used this traffic to harvest credit card and other personal information, for use in the commission of online identity fraud. For this reason, the online payments industry has engaged closely with law enforcement to combat this illicit traffic. Major credit card companies and banks in the US, Europe and

the Far East have been collaborating with law enforcement through financial coalitions to close down their systems to this type of crime.[58] Disrupting the business model in this way has reduced the commercial distribution of child sexual abuse material.

Citizens

Mechanisms for citizens to report child sexual abuse material are used to manage such content. These kinds of tools require the user to be proactive in reporting child sexual abuse material regardless of the jurisdiction in which it was produced and distributed and serves to create a sense of community to manage and moderate such material. For example, the EU has supported and developed member states alert platforms and a Europol Alert Platform for reporting offences on the internet.

Conclusion

Complex cross-border regulatory problems are increasingly requiring collaboration between different industries and sectoral regulators to produce an effective response. Child sexual abuse material is an example of the involvement of other sectors, such as communications and finance, to assist law enforcement.

There are several international conventions providing a framework to address child sexual abuse material, as well as several law enforcement organisations that facilitate collaboration with law enforcement agencies. For example, the ACMA is a participant in INHOPE.

As well as individual companies, industry bodies have contributed tools to combat the proliferation of child sexual abuse material. Tools include enabling reporting of online child sexual abuse material, blocking IP addresses and collaborating with law enforcement agencies. In addition, there are several mechanisms for reporting child sexual abuse material available to citizens.

[58] Examples include the Financial Coalition against Child Pornography that involves over 30 major banks and other institutions in the online payments industry. Its goal is to eradicate the profitability of commercial child pornography by shutting down payments accounts that are being used by illegal enterprises. In Canada, Cybertip is working with payment providers and financial institutions to track and eliminate payment options.

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 44
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

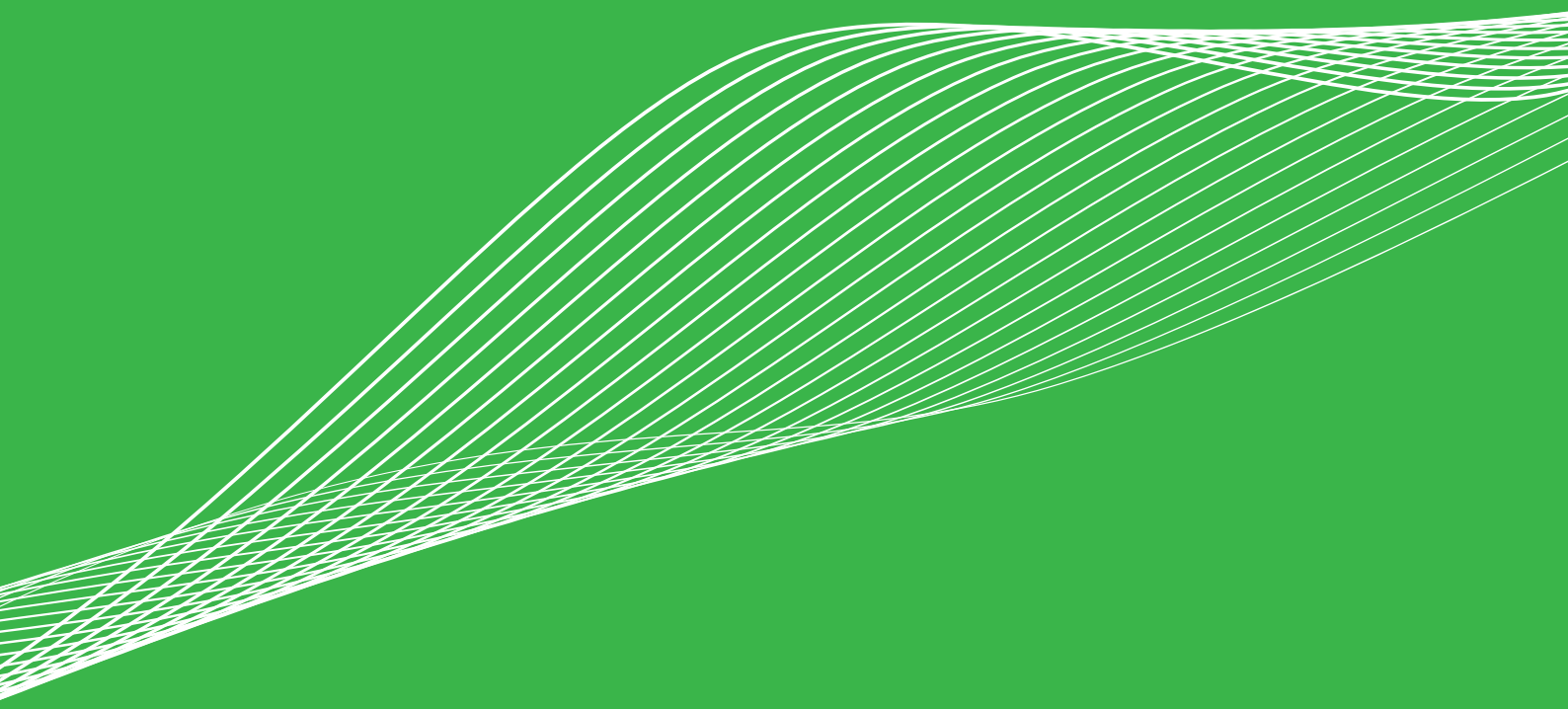
T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
1800 226 667
F +61 2 9334 7799

researchacma



acma.gov.au