California Pioneers New Law to Protect Young People from Online Privacy and Advertising Abuses

Dr. Alana Maurushat, David Vaile and Carson Au examine recent reforms to the law in California regarding the privacy of minors and consider whether Australia should enact similar provisions.

Introduction

Governments face a number of issues with youth, online technologies and privacy. Children are sending one another provocative and sexualized self-images ("sexy selfies") and violent content via SMS, Facebook, Snapchat and other social networks, without realising the potential consequences. Companies are collecting vast amounts of data from minors without adequate consent. Advertisers are using social network sites to market in a fashion not otherwise permitted in the offline world.

While many jurisdictions have attempted to tackle these privacy issues using educational campaigns and longstanding privacy principles, other jurisdictions such as California have proposed new online privacy bills dedicated to children. This article examines two recently proposed California privacy bills and discusses whether Australia should consider enacting similar provisions.

Companies are collecting vast amounts of data from minors without adequate consent

California Bills

Two Californian Senate Bills were introduced in 2013 concerning, children and digital privacy: Senate Bill 501[1] (***Social Networking Privacy Act*** *or* ***SB 501***) and Senate Bill 568[2] (***Privacy Rights for California Minors in the Digital World*** *or* ***SB 568***).

The Social Networking Privacy Act (SB 501)

The California Senate has passed SB 501, but it still remains in the Assembly as of February 2014. SB 501 applies to both adults and minors (those under 18 years of age) residing in California. It requires 'a social networking Internet Web site to remove the personal identifying information of a registered user that is accessible online'[3] within 96 hours upon request of the user.[4] A registered user means any persons who have created an account for the purpose of accessing the social networking site.[5] However, for users who are minors, the site is also required to remove the content upon the request of the parent or legal guardian of the minor.[6]

The obligation to remove personal information is imposed on social networking Internet Web sites, which are expressly defined as 'service[s] that allow an individual to construct a public or partly public profile within a bounded system, articulate a list of other users with whom the individual shares a connection, and view and traverse his or her list of connections and those made by others in the system'.[7] Since the word 'connection' is not defined, the scope is broad and is not limited to services such as Facebook and Twitter. For example, it is arguable that YouTube, a website primarily for videos, falls within the scope of this definition because it enables users to connect to other users by subscribing or commenting on another user's video. The user can additionally click on the profiles of other users and browse through the connections that the user has made (e.g. the videos that he or she has commented on). An e-commerce site that enables customers to review products and comment on other customer's reviews and browse other customer's profiles and previous product reviews, would similarly fall within this scope.

The bounds of 'personal identifying information' are expressly limited to a person's:

street address;
telephone number;
driver's license number;
state identification card number;
social security number;
employee identification number;
mother's maiden name;
demand deposit account number;
savings account number; or
credit card number.

There are clearly a range of data items potentially useful for effectively identifying individuals which are not covered, including inter alia other forms of financial system identifiers, other account names, identifiers including nicknames, and technical identifiers such as those broadcast by a child's mobile phone or computer or inserted by way of tracking technologies onto their device.

SB 501 imposes a civil penalty of no more than US$10,000, for each wilful and knowing violation.[8]

The primary criticism of SB 501 is that it burdens the free expression of minors. Parents of children would be able to request the removal of any social networking posts of their children.[9] Additionally, because of the inherent difficulty of verifying identity on the

1 Sen. Bill No. 501 (California) http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB501
2 Sen. Bill No. 568 (California) http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568
3 Sen. Bill No. 501 § 60(a)
4 Sen. Bill No. 501 § 62(a)
5 Sen. Bill No. 501 § 62(c)
6 Sen. Bill No. 501 § 62(a)
7 Sen. Bill No. 501 § 62(c)
8 Sen. Bill No. 501 § 65
9 Llanso, E 2013, 'Comments on SB 501: The Social Networking Privacy Act and SB 568, Regarding Privacy Rights for California Minors in the Digital World', *Center for Democracy & Technology,* viewed 28 November 2013, <https://www.cdt.org/files/pdfs/CDT-Testimony-SB501-SB568.pdf>

Internet, SB 501 may be subject to abuse.[10] SB 501 may also impose a significant burden on operators, which may lead to operators banning minors from using their products and services.

Privacy Rights for California Minors in the Digital World (SB 568)

SB 568 was signed into Californian law on 23 September 2013 and will take effect on 1 January 2015 as *California Business and Professions Code* § 22580-82. SB 568 imposes obligations with respect to advertising and content removal.[11] ReedSmith has published a useful flowchart explaining the application of SB 568,[12] which is summarised below.

The content removal obligations imposed by SB 568 apply to operators of Internet Web sites, online services, online applications or mobile applications 'directed to minors'[13] where the operator has actual knowledge that a minor is using its services. The phrase 'directed to minors' is defined as having 'the purpose of reaching an audience that is predominantly comprised of minors, and is not intended for a more general audience comprised of adults'.[14] This definition is vague. For instance, cartoon mobile games such as Angry Birds may arguably have been intended for audience that is predominantly minors. However, since the game has become popular with adults, it is also arguable that it is intended for a more general audience. The 'actual knowledge' requirement does not require operators to inquire about the user's age.[15] Subsequently, operators can avoid liability by not collecting age information or by banning minors upon obtaining such information.

Such operators must notify registered users who are minors of their right to request and to obtain removal of content posted on the operator's Internet site, service or application by the minor.[16] Clear instructions on this procedure must also be provided.[17]

Nevertheless, there are exceptions where the operator is not obliged to remove the content upon request. Notably, if the content at issue is posted by a third party, even if the content was a re-publication or a re-post of the aggrieved minor's initial post, the operator is not obliged to remove the content.[18] This will also be the case where the operator de-identifies the content such that the minor cannot be individually identified or if the minor has received compensation or consideration for the content.[19] Furthermore, an operator is deemed to have complied with SB 568 if the original posting was made invisible to the public, even if the content remains visible because it has been copied or re-posted by a third party.[20]

These exceptions may render the practical application of SB 568 ineffective, especially given that in many cases, the more embarrassing the post, the more likely it is to be shared by third-parties.[21]

SB 568 imposes advertising restrictions on operators of Internet Web sites. For example, if an operator of an Internet Web site, online service, online application or mobile application is 'directed to minors', then under SB 568 they will be prohibited from marketing or advertising goods and services listed in § 22581(i).[22] Examples include firearms and alcoholic beverages. The operator is not required to have actual knowledge that minors are users.

Alternatively, a similar operator who has actual knowledge of minors using its site, service or application (regardless of whether it is 'directed to minors') is prohibited from marketing or advertising the § 22581(i) goods and services to the minor if the marketing or advertising is based upon information specific to that minor.[23]

While many jurisdictions have attempted to tackle these privacy issues using educational campaigns and longstanding privacy principles, other jurisdictions such as California have proposed new online privacy bills dedicated to children

Finally, if a similar operator has actual knowledge of minors using its site, service or application, or has actual knowledge that the site, service or application is 'directed at minors', the operator shall not knowingly (or allow a third party) 'use, disclose, compile ... the personal information of a minor with actual knowledge' that it is for the purposes of marketing or advertising the § 22581(i) goods and services to that minor.[24]

SB 568 has been criticized on a number of grounds including vagueness of law, its ineffectiveness, its over-ambition and its potential loopholes. Eric Goldman, a Professor of Law at Santa Clara University School of Law, highlighted several uncertainties,[25] which are set out below.

---

10 Above, n8 at 1.

11 Goldman, E 2013, 'California's Latest Effort To 'Protect Kids Online' Is Misguided and Unconstitutional', *Forbes - Eric Goldman – Tertium Quid blog, 24* September, viewed 28 November 2013, <http://www.forbes.com/sites/ericgoldman/2013/09/30/californias-latest-effort-to-protect-kids-online-is-misguided-and-unconstitutional/>

12 ReedSmith 2013, *Reference Guide to SB 568 – Internet Privacy For California Minors*, ReedSmith, viewed 28 November 2013, <http://www.globalregulatoryenforcementlawblog.com/uploads/file/Internet%20Privacy%20for%20CA%20Minors%20-%20Reference%20Diagram_phcho.pdf>

13 Sen. Bill No. 568 § 22581(a)

14 Sen. Bill No. 568 § 22580(e)

15 Sen. Bill No. 568 § 22581(e)

16 Sen. Bill No. 568 § 22581(a)

17 Sen. Bill No. 568 § 22581(a)

18 Sen. Bill No. 568 § 22581(b)

19 Sen. Bill No. 568 § 22581(b)

20 Sen. Bill No. 568 § 22580(d)

21 Karohonik, T 2013, 'Why California's new online privacy bill will cause more problems than it solves', *New Media Rights*, 25 September, viewed 28 November 2013, <http://www.newmediarights.org/that%E2%80%99s_great_idea%E2%80%A6_pity_it_won%E2%80%99t_work_look_why_california%E2%80%99s_new_online_privacy_bill_will_cause_more>

22 Sen. Bill No. 568 § 22580(a)

23 Sen. Bill No. 568 § 22580(b)

24 Sen. Bill No. 568 § 22580(c)

25 Goldman, E 2013, 'California's New 'Online Eraser' Law Should be Erased', Forbes - *Eric Goldman – Tertium Quid blog*, 24 September, viewed 28 November 2013, <http://www.forbes.com/sites/ericgoldman/2013/09/24/californias-new-online-eraser-law-should-be-erased/>

First, for SB 568 to apply to an operator, the operator's website or app must be 'directed' to minors. It is difficult to distinguish between content aimed at young adults, and content aimed at 17 year olds. Many websites such as Instagram, or apps such as Angry Birds are popular with both minors and young adults. [26]

Second, SB 568 provides that the minor has the right of removal, but does not define when the minor can exercise the removal right. It is unclear whether an adult will have the right of removal for content initially posted when they were a minor. If not, the law would then require minors to make arguably mature and adult decisions (that is, on what content they wish to keep in the public for the rest of their lives) whilst being still minors.

Third, the advertising restrictions do not define 'personal information,' nor does it explain what constitutes an 'advertising service'.

SB 568 only provides the right of removal of the initial post by the user. If the post is copied to another site, or shared by another user, no right of removal will exist. This is particularly problematic as the more embarrassing a post or a photo is, the more likely that it is to be shared. [27]

SB 568 has been criticized on a number of grounds including vagueness of law, its ineffectiveness, its over-ambition and its potential loopholes

SB 568 only imposes burdens on operators with actual knowledge of minors using its products and services. By not collecting age information at all, websites are able to escape the operation of this law. [28]Further, SB 568 does not state that the content removal mechanism has to be automated. It only requires that it is available. By making the mechanism sufficiently difficult to use, slow or onerous (e.g. by requiring users to request removal via physical mail), the operator may be able to significantly reduce such requests. [29]

While there are plenty of criticisms of both SB 501 and SB 568, there is merit to the argument that something needs to be done to safeguard minors' privacy online. It is a useful contribution to regulation addressing online harms suffered most acutely by young people.

The Australian Framework

Privacy issues relating to youth and social networking sites are not regulated separately in Australia but are instead included within the general scope of privacy law under the Australia Privacy Principles (***APPs***), which take effect on 12 March 2014. These ten principles are:

APP 1: open and transparent management of personal information
APP 2: anonymity and pseudonymity
APP 3: collection of solicited personal information
APP 4: dealing with unsolicited personal information
APP 5: notification of the collection of personal information
APP 6: use or disclosure of personal information
APP 7: direct marketing
APP 8: cross-border disclosure of personal information
APP 9: adoption, use or disclosure of government related identifiers
APP 10: quality of personal information
APP 11: security of personal information
APP 12: access to personal information
APP 13: correction of personal information

There is no general common law or statutory right to privacy in Australia, although the latter is under consideration by the Australian Law Reform Commission. This means that if a young person falls through this regime there is often little in the way of a remedy.

SB 501 and SB 568 offer a list of 'personal identifying information' which include a person's street address, telephone number, and so forth, consistent with other US usage. Australian law, in keeping with other OECD practice, uses a broader definition of 'personal information.' Under section 6 of the *Privacy Act 1988* (Cth) (the ***Privacy Act***), 'personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

Information from which identity "can reasonably be ascertained" potentially extends quite broadly, focusing on the function of identification (which can change with developments in business process or data handling, such as the Big Data capabilities for re-identification of previously de-identified or anonymised records) rather than a fixed list of identifiers which represent only a subset of data items useful for identification purposes.

However, section 16 of the Privacy Act exempts personal, family or household affairs, consistent with the Act's original focus on business and government records:

> Nothing in the Australian Privacy Principles applies to: (a) the collection, holding, use, disclosure or transfer of personal information by an individual; or (b) personal information held by an individual; only for the purposes of, or in connection with, his or her personal, family or household affairs.

The commissioner rarely makes determinations, so there is in effect no body of law about interpretation of such provisions, but it is clearly open to treat most communications between individuals about their "personal affairs" as in effect outside the scope of the Privacy Act. Most of the relevant actions are thus undertaken by people outside the ambit of the Privacy Act, or potentially within it but outside the jurisdiction.

In the context of online social networking sites (most of which are operated or owned by businesses incorporated in America using American law, as per the applicable in the terms and conditions), but in some cases potentially subject to Australian consumer protection law), and in the absence of a general enforceable right to privacy in Australia, the Privacy Act plays a small role. If for example, a minor or a minor's guardian wished to have personal information removed from a minor's Facebook account, they could request that Facebook (for example) remove the content. Facebook has no legal obligation absent a court order to remove any content. The decision lies with the online social network. While the Australian privacy framework is available to the minor, it would require a formal complaint to be made to the Privacy Commissioner, who may look into the issue, decide to investigate and then render a decision within two months to ten years. During this process, the Commissioner may meet with the online social network provider and advise as to how to best change practices to prevent future privacy breaches, if indeed a privacy breach was even present. This framework, given the low rate of determinations made over the years and the slow response time[30] compared to the high volume of rapidly shared unwanted publications about young people, is largely irrelevant for many of the real problems with personal identification information, social network sites and minors (and adults as well).

---

26 Above, n19 at 5.

27 Above, n19.

28 Above, n19.

29 Above, n19.

Advertising and marketing is regulated in Australia. Each State has its own codes and regulations affecting advertisers and marketers, and the *Competition and Consumer Act 2010* (Cth) (embodying the Australian Consumer Law) likewise applies throughout Australia. Australian consumer law covers some main areas related to advertising including: misleading and deceptive conduct; false or misleading representations; unconscionable conduct; representations about country of original, and information standards. These statutes, however, do not expressly contain any provisions specific to marketing and advertising to minors, and the extent to which they apply to online services remains ambiguous.

It is unclear whether an adult will have the right of removal for content initially posted when they were a minor

The area is additionally self-regulated by the Advertising Standards Bureau who 'administers a national system of advertising self-regulation through the Advertising Standards Board and the Advertising Claims Board.'[31] Online marketing and advertising to minors using social network sites has two distinct advantages. First, there are no laws or regulations specific to minors. Second, as most online social network sites are American, Australian law has little to no extra-territorial effect (though the effect of the Australian Consumer Law can be seen in Australian-specific clauses, drawing attention to non-excludable protections, in licences from offshore online entities like Adobe and Apple). While a party could complain to the appropriate regulatory authority such as the ACCC, the chances of obtaining an effective remedy are slim to none, unless there is an Australian presence.

Conclusion

California has been a pioneer of modern privacy law with the first introduction of mandatory data breach notification legislation, a very powerful spam law in 2003 (sadly over-ridden by the spam friendly federal CAN-SPAM Act of 2003), and now reforms addressing privacy, online technologies and minors. There are clear issues here which require action but sometimes the best approach is to wait and see. If California successfully enacts SB 501 and SB 568, there will be ample evidence within a few years of their operation as to their effectiveness and problematic components. If enough jurisdictions begin to legislate in the area, large companies such as Facebook and WhatsApp may begin to self-regulate so that their internal practice will reflect stricter more protective practice as required under the law. Some corporations may also choose to comply with the most stringent privacy law from one significant jurisdiction (eg. Europe) as opposed to having different technical platforms and marketing practices in every jurisdiction that they operate. In the aftermath of recent concerns over data sovereignty, this effect may grow stronger in the near term.

Dr Alana Maurushat, David Vaile and Carson Au are members of the Cyberspace Law and Policy Community, Faculty of Law, at the University of New South Wales.

---

30 Connolly, C and Vaile, D. Communications privacy complaints: in search of the right path, Cyberspace Law and Policy Centre, UNSW, 14 September 2010 <http://cyberlawcentre/org/privacy/ACCAN_Complaints_Report/report.pdf> .

31 Advertising Standards Bureau, http://www.adstandards.com.au/aboutus/aboutselfregulation.

CAMLA's Young Lawyers Event 2014 - Another 'Sell Out'!

CAMLA's second event for young and junior lawyers was held on 11 February 2014 at Baker & McKenzie in Sydney and was well oversubscribed and attended!

Organised by CAMLA's Young Lawyers Committee, the evening took a light-hearted panel format comprising Toby Ryston-Pratt (Deputy Chief Legal Counsel, NBN Co), John Corker (Visiting Fellow, UNSW), Andrew Stewart (Partner, Baker & McKenzie), and Sandy Dawson (Barrister, Banco Chambers) and was moderated by Ryan Grant (Senior Associate, Baker & McKenzie). The panellists provided the audience with fascinating insights into their career journeys so far and advice to young lawyers as to where their law degrees and experience may take them.

The event also included the presentation of awards for the prize-winners in the CAMLA essay competition. Prizes were awarded to Jarrod Bayliss-McCulloch of Baker & McKenzie for his essay entitled "Does Australia need a 'right to be forgotten' ?", Kanin Lwin of The University of Sydney for his essay entitled "Australia's Privacy Principles And Cloud Computing: Another Way" and to Michael Douglas of The University of Western Australia for his essay entitled "Intervention of Media Organisations in First Instance Proceedings: A Matter of Natural Justice". The essays were judged by representatives of private practice, industry and academia. Awards were announced and presented by CAMLA President, Page Henty.

By all reports the panel presentation, synopses of prize winning essays (and of course plentiful refreshments) we enjoyed by all, with many looking forward to the next event. Particular thanks must go to each of the panellists for their time, insights and advice, and to Baker & McKenzie for hosting the event.

Stay in touch with CAMLA via our website (www.camla.org.au) and LinkedIn page for news on upcoming CAMLA events, the bulletin and membership information.