Date of Hearing: June 25, 2013

ASSEMBLY COMMITTEE ON ARTS, ENTERTAINMENT, SPORTS, TOURISM, AND INTERNET MEDIA
Ian C. Calderon, Chair

SB 501 (Corbett) – As Amended: June 5, 2013

SENATE VOTE: 23-10

SUBJECT: Social networking Internet Web sites: privacy: minors.

SUMMARY: Requires a social networking Internet Web site, as defined, to remove the personal identifying information, as defined, of any registered user that is accessible online, within 96 hours after his or her request and would also require removal of that information in that same manner regarding a user under the age of 18 upon request by the user's parent or legal guardian. This bill would not require removal or elimination of the personal identifying information if federal or state law otherwise requires the social networking Internet Web site to maintain the information. Specifically, this bill:

1) Provides that a social networking Internet Web site shall remove the personal identifying information (PII), as defined, of a registered user, as defined, that is accessible online in a timely manner upon his or her request.

2) Further provides that in the case of a registered user who identifies himself or herself as being under 18 years of age, the social networking Internet Web site shall also remove the information upon the request of a parent or legal guardian of the registered user.

3) Declares that a request submitted by a registered user shall include sufficient information to verify the identity of the user and shall specify any known location of the information that is the subject of the request.

4) Requires that a social networking Internet Web site may require a request to include the following statement:

   "I attest that the information in this request is accurate, that I am the registered user or the parent or legal guardian of the registered user to whom the personal identifying information in this request pertains, and that I am authorized to make this request under the laws of the State of California."

5) Provides that a social networking Internet Web site is not required to remove or otherwise eliminate personal identifying information if any other provision of federal or state law requires the Internet Web site to maintain the information.

6) Declares that its provisions shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from a social networking Internet Web site as authorized by law or pursuant to an order of a court of competent jurisdiction.

7) Provides the following definitions:

   a) "In a timely manner" means within 96 hours of delivery the request.

   b) "Personal identifying information" means 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.

   c) "Registered user" means any person who has created an account for purposes of accessing a social networking Internet Web site.

   d) "Social networking Internet Web site" means an Internet Web-based service that allows 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.

8) Provides that a social networking Internet Web site that willfully and knowingly violates any provision of this part shall be liable for a civil penalty, not to exceed ten thousand dollars ($10,000) for each violation of this part.

9) Declares that nothing in this part shall be construed to allow the imposition of a civil penalty for an unintentional violation.

EXISTING LAW:

1) Provides that, among other rights, all people have an inalienable right to pursue and obtain privacy. (California Constitution, Article I, Section 1.)

2) Permits a person to bring an action in tort for an invasion of privacy and provides that in order to state a claim for violation of the constitutional right to privacy, a plaintiff must establish the following three elements:

   a) A legally protected privacy interest;

   b) A reasonable expectation of privacy in the circumstances; and

   c) Conduct by the defendant that constitutes a serious invasion of privacy. [*Hill v. National Collegiate Athletic Assn.* (1994) 7 Cal.4th 1.] Existing law recognizes four types of activities considered to be an invasion of privacy giving rise to civil liability, including the public disclosure of private facts. (*Id.*)

3) Provides that there is no reasonable expectation of privacy in information posted on an Internet Web site. The information is no longer a "private fact" that can be protected from public disclosure. [*Moreno v. Hanford Sentinel* (2009) 172 Cal.App.4th 1125.]

4) Requires an operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in

California who use or visit its Web site to conspicuously post its privacy policy. (Online Privacy Protection Act of 2003, Business & Professions Code Section 22575.)

5) Existing federal law makes it unlawful for an operator of a Web site or online service directed to children under the age of 13 to collect personal information from a child, including a child's first and last name, home or other physical address including street name and name of a city or town, e-mail address, telephone number, or Social Security number. (Child Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et. seq.)

FISCAL EFFECT: None

COMMENTS:

1) Author's Stated Need for Legislation:

According to the author, "Computer systems and the Internet have brought consumers many conveniences. But these innovative methods of information sharing can pose a serious threat to our privacy and security. There are countless privacy pitfalls when our personal identifying information is indiscriminately posted.

"Current law does not require a social networking Web site to honor a user's request or, in the case of a minor user under the age of 18, a parent or legal guardian's request to remove certain personally identifiable information (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).

"This bill is the next logical step in protecting a user's personal identifying information. The ability to request the removal of personal identifying information from a social networking website allows a user to protect him or herself. In the case of a user who is a minor under the age of 18, it provides a parent or legal guardian with a reasonable and logical tool to protect their children from the dangers of making personally identifiable information available online."

2) Background: Social Media and Minors:

Social networking Internet Web sites such as MySpace and Facebook have grown in use and become more popular with users who post messages and photos on a personal web page. Those personal pages, generated by the social networking Web site, may also display the user's address, phone number, birth date, or other personal identifying information. That information may then be displayed to the user's friends or to the general public. Although users may limit who may see their personal information, many users, including those under the age of 18, often share that information with their "friends." The list of "friends" for those users may include people who they do not personally know, resulting in the sharing of personal identifying information with unknown persons.

Children under the age of 18 are among the most avid users of social networking Internet Web sites. A report by the Pew Foundation entitled *Social Media & Mobile Internet Use Among Teens and Young Adults* (February 2010) found that 93 percent of American teens

between the ages of 12 and 17 are online, and that 73 percent of these teens use social networking sites. (*See* http://www.pewinternet.org/Reports/ 2010/Social-Media-and-Young-Adults.aspx, as of April 20, 2013.) A 2005 survey by the Polly Klaas Foundation found that 42 percent of online teens post information about themselves on the Internet so others can contact them, and 56 percent have been asked personal questions online. (Polly Klass Foundation, *Omnibuzz Research Poll Results*, http://www.pollyklaas.org/internet-safety/internet-pdfs/PollingSummary.pdf, as of April 20, 2013.) Additionally, 10 percent of children aged 8-12 surveyed said they communicate online with people they don't know. (*See id*.)

Many research organizations have found that the sharing of personal identifying information through social networking Internet Web sites poses a significant threat to personal privacy. A 2010 Consumer Reports survey found that, "Many social network users are naive about risks. Forty percent had posted their full birth date, exposing them to identity theft. Twenty-six percent of Facebook users with children had potentially exposed them to predators by posting the children's photos and names. And in one of four households with a Facebook account, users weren't aware of or didn't choose to use the service's privacy controls." (Consumer Reports, *Social insecurity: What millions of online users don't know can hurt them*, http://www.consumerreports.org/cro/magazine-archive/2010/june/ electronics-computers/social-insecurity/overview/ index.htm, as of April 20, 2013.)

Social network users under the age of 18 are particularly at risk. According to the American Academy of Pediatrics (AAP), "[t]he main risk to preadolescents and adolescents online today are risks from each other, risks of improper use of technology, lack of privacy, sharing too much information, or posting false information about themselves or others." (AAP, *The Impact of Social Media on Children, Adolescents, and Families*, http://pediatrics.aappublications.org/content/127/4/800.full, as of April 20, 2013.) "These types of behavior," according to the AAP, "put [minors'] privacy at risk." (*Id*.)

The posting of too much information may be unintentional, or in some cases the result of unfamiliarity with a particular Web site or confusion about how information will be displayed across a social network. A study by Columbia University entitled *The Failure of Online Social Network Privacy Settings* found that 93.8 percent of participants revealed information that they intended to keep private, and that 84.6 percent of participants were hiding information that they actually wanted to share. (http:// academiccommons. columbia.edu/catalog/ac:135406, as of April 20, 2013.)

This over-sharing and confusion has contributed to an environment where 92% of parents are concerned that their children shared too much information online, and 75% of parents don't think social networking sites do a good job of protecting children's online privacy. (Common Sense Media, *Common Sense Media Poll*, http://www.commonsensemedia.org/sites/default/files/ privacypoll.pdf, as of April 20, 2013.)

3) Tragedy, Federal Trade Commission (FTC) Privacy Actions and Maturity Bring Changes to Social Network User Information Practices:

In 2006, according to a CBS News story, 14-year-old Judy Cajuste was murdered in New Jersey, after she reportedly told friends she met a man in his 20s through MySpace.com. Across the country, in Northern California, 15-year-old Kayla Reed was also active on

MySpace until the day she disappeared. The Center for Missing and Exploited Children revealed that in 2005, there were more than 2,600 incidents of adults using the Internet to entice children.

To test the dangers posed to children in the online community, that same year "Wired News" ran the names of randomly selected registered sex offenders in San Francisco and neighboring Sonoma County through MySpace's user search engine and turned up, "no fewer than five men whose self-reported names, photographs, ages, astrological signs, locations and (in two instances) heights matched those of profiles on the state's online sex offender registry."

The social networking community responded to these safety issues. In order to prevent online solicitation of its members, MySpace developed and implemented a program called "Sentinel Safe" which allows them to aggregate all publicly available sex offender databases into a real-time searchable form, making it easy to cross-reference and remove known registered sex offenders from the MySpace community. In February of 2009, MySpace revealed that 90,000 registered sex offenders have been identified and kicked off its site in the past two years using this technology.

Chris Kelly, Facebook's then-chief privacy officer stated at the time that, "We have devoted significant resources to developing innovative and complex systems to proactively monitor the site and its users, including those not on a sex offender registry, for suspicious activity (such as contacting minors or users of predominantly one gender). We also have established a large team of professional investigators to evaluate any reports of potential abuse, including those surfaced by our systems or from our users."

During approximately this same period of time, 2006-08, the FTC began a series of enforcement actions against social network sites, alleging that they did not follow their stated privacy policies and misled users as to the control and use of their personal identifying information. The charges include collecting information provided by users gathered from their registration information and user activities (such as "likes" and pictures); sharing user information with third party applications for marketing purposes, and; making misleading changes to their privacy policies which intentionally obscured and broadened their information gathering practices. As a result of these enforcement actions, Facebook, Google and MySpace (and others) each signed settlement agreements with the FTC and agreed to follow their privacy policies and to annually submit their privacy policies and share any changes with the FTC for 20 years. In addition, the networks subject to the settlement agreements must now "clearly and prominently" disclose to the users sharing of their personally identifying information beyond that declared in the privacy policy, and must have the user's affirmative consent prior to any sharing of user's PII.

One outcome of the FTC settlements was a task force of industry and state Attorneys General, who convened in 2008. Their task for the report, *Enhancing Child Safety & Online Technologies*, (Task Force Report) established best practices for operators in the social network environment.

As a partial result of the activities above, MySpace established parental controls which allow the parents of teens to monitor their child's MySpace activities, and to remove the MySpace page of their child. Facebook and Google also changed their privacy settlings for youth and

child users, limiting information children and teens may access and the scope of users who may contact teens and children to those users also known to be minors.

The social network community now has adopted many of the child safety practices contained in the Task Force report for users who identify themselves as minors.

4) Constitutional Right to Personal Information Privacy:

Both the federal and state constitutions provide protection for individuals' privacy. Unlike the federal Constitution, California's constitution explicitly recognizes a right to individual privacy in its text, stating "All people are by their nature free and independent and have inalienable rights. Among these are ... pursuing and obtaining safety, happiness, and privacy." (California Constitution, Article 1 Section 1.)

The leading case regarding a private right of action under the California constitution against a private entity for a violation of privacy rights is *Hill v. Nat'l Collegiate Athletic Ass'n, 26 Cal. Rptr. 2d 834, 857 (Cal. 1994).* In *Hill*, the California Supreme Court recognized that the California constitution's right of privacy creates a private right of action, not only against the government, but also non-governmental entities.

The Court further held that the California constitutional right to privacy protects two types of privacy; anatomical or physical privacy, and informational privacy, which the court defined as protecting interests in "precluding the dissemination or misuse of sensitive and confidential information." Id.

In *Hill*, the California Supreme Court relied upon the ballot argument for Proposition 11, a.k.a. the Privacy Initiative, which urged the need for greater protection against the potential misuse of information gathered by both government and private entities. The ballot argument raised the concern that the government and private entities might use that information for other objectives not related to the original purpose of gathering the information. The ballot argument also raised the concern that information gathered by the government and non-governmental entities would be used to "embarrass" individuals. Id.

"As the argument in favor of Proposition 11 observes: 'At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian. The right of privacy prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. The proliferation of government and business records over which we have no control limits our ability to control our personal lives.' …" *Hill*, id.

This measure would expand upon the right to privacy by allowing registered users of Internet social networks to remove personally identifying information which they object to being made public from the site, or in the case of parents, the personal information of their minor children.

5) Arguments in Support:

a) The Internet Provides a Unique Environment for Predators to Contact Child Victims:

The Klass Foundation offers the following which is typical of other supporters for this bill, stating, "Cybercrime against children represents a criminal phenomenon unique to the 21st Century. The days of monitoring your kid's online activity by putting the home computer in the living room are long past, because cell phones, PDA's, wireless laptops, and libraries all offer easy Internet access. Therefore, we must find other means to protect children from predatory behavior on the Internet.

"Children used to beware predators lurking in alleys, dark stairwells, in and around parks and schoolyards. The Internet has emboldened a new generation of cyber-perverts who rely upon anonymity and subterfuge to engage their evil intentions. This small subset lurks behind false profiles as they attempt to lure, groom, and victimize our children. The very predators who cannot penetrate our dead bolts, alarm systems, guard dogs, or personal armories have found a back alley into our living rooms under the camouflage of binary code and new world technology."

b) Children and Teens Need "Hind-sight" Privacy Protections:

Common Sense Media adds in their support, "This common sense measure is especially important for kids and teens. Teenagers are using social networking sites such as Facebook and Twitter in extraordinary large numbers. According to a recent study, nine out of 10 (90%) 13 to 17-year-olds have used some form of social media. Additionally, three out of four (75%) teenagers currently have a profile on a social networking site and 68% of all teens say Facebook is their main social networking site. While these sites offer a myriad of benefits, such as allowing users to easily connect with family and friends and share information, they also pose risks. Children and teens often reveal before they reflect, and may post personal information, such as addresses, telephone numbers and even social security and account numbers, without realizing the consequences. Kids do not necessarily understand that identity thieves and other malicious individuals can access and exploit this sensitive personal information."

"This bill addresses this critical privacy issue head-on by requiring social networks to comply with users' requests to remove their personal identifying and financial account information. There are enormous risks when our personally identifiable information is indiscriminately posted, indefinitely stored, and quietly collected and analyzed by marketers and ID thieves. Those risks are especially serious when it comes to kids and teens, who are tracked more closely and widely than adults."

c) Parents Desire the Ability to Protect Their Children Online:

According to a recent Common Sense Media poll:

94% of parents say they should be able to request the deletion of all their personal information held by a search engine, social network, or marketing company after a specific period.

75% of parents don't think social networking sites do a good job of protecting children's online privacy.

85% of parents say they are more concerned about online privacy than they were five years ago.

d) Teen Dating Violence is Often Reflected in Online Behavior:

The Partnership to End Domestic Violence also supports this measure for a different reason writing to say, while technology is an integral part of our lives, and social networking sites are used by millions, "What is often unrecognized however are the ways in which technology can be misused and place victims of domestic violence in extreme danger. In particular teen dating violence often intersects with the digital world, where technology is often used as a tool for abuse. This bill provides another tool teens can use to protect their privacy."

6) Arguments in Opposition:

a) SB 501 Would Violate Free Speech Rights of Minors:

A majority of opponents to this bill raise concern with the provision of the bill permitting parents to require removal of their children's personal identifying information, claiming it presents significant First Amendment concerns. This line of argument is typified by the Electronic Frontier Foundation (EFF), who state in their opposition, "This bill would allow parents or legal guardians to require social networks to remove the personal identifying information of their minor children, defined as those under the age of 18, upon request. As we read the bill, parents or legal guardians may exercise this power in conflict with their minor children's wishes, permitting them to restrict their children's speech and association on social networks. EFF believes that minors have First Amendment rights to speak and associate, especially adolescents or teenagers, who have significant need to discuss issues such as reproductive health, sexual orientation, lifestyle, religion, politics, and culture. The sensitivity of these issues makes the possibility of disagreement over social network speech and association real. As a result, the bill places state power behind likely parental or guardian censorship, and raises grave First Amendment concerns."

b) Creates Incentive for Minors to Lie About Their Age, Increasing Their Online Risks:

According to a letter signed jointly by many members of the technology industry (Joint Letter of Opposition), "Many social networking sites ask for users' dates of birth for one important reason: to protect users that identify themselves as under 18. Once a user is identified as a minor, a number of behind-the-scenes security measures kick in. These range from restrictions on adults being able to search for minors, limits on minor's ability to share information with strangers, and additional steps in the friend verification process. Additionally, by default, access to contact information is limited to friends only.

"All of the additional protections social networks can provide for minors are dependent on the minor accurately representing her age. By denying minors the ability to publish data entered into text fields designated for phone and address information, this bill may

encourage minors to lie about their age to restore the lost functionality, this would enable them to circumvent the restrictions of this bill while undermining existing privacy and security protocols."

c) Creates a False Sense of Safety and Addresses the Wrong Harm:

The Family Online Safety Institute and Stop Child Predators are concerned that, "By diverting attention to restricting the display of home addresses and telephone numbers - instead of real online threats such as cyberbullying and grooming - this bill could actually increase the risk to minors by creating a false sense of security among both minors and parents. Parents should not be encouraged to believe that restricting the display of this type of information will somehow make children safer, when in fact, attention needs to be focused on more credible threats."

d) Increases Risk of Identity Theft:

Various opposition groups asserted that the information gathering necessary to comply with the verification requirements of this bill could have the unintended consequence of creating a data base of PII which would be very attractive to identity thieves. Typical of this concern is that voiced by iKeepSafe, who write to say that an "unexpected outcome of this bill is that social networking sites will gather and review more personal and confidential information about their young users and their families and potentially their guardian's family. … Determining guardianship and custodial responsibilities will require that even more sensitive information will be gathered and shared with industries like Facebook and Google only increasing risks to family and youth."

7) Committee Staff Drafting Issues:

This bill, as written, contains a number of provisions which committee staff believe may pose implementation and/or interpretation issues were the measure to become law.

a) Recent amendment language which added "that is accessible online" may have created a duty for the social networks to search the entire Internet for places where PII of the registered user occurs. However, Social networking sites (SNS) only have control over their own sites. This language created a substantial burden for SNS to search for the information subject to a removal request everywhere on the Internet - and potential liability for any site where the PII remains available, despite the inability of the SNS to remove the information from an unrelated Internet site.

b) Language which triggers the provisions of this bill for minors hinges on the self-reported age of the registered user as being under 18; given that the Pew Foundation report that 44% of minors who are social network users admit they lie about their age, this reliance seems misplaced. Also, if a child can subvert the intent of the legislation by simply changing their age status to 18 and above, this language would seem to encourage savvy minors to misstate their age to avoid its application to them.

c) Language in the bill which requires SNS to remove the PII of registered users from "any known" location is not sufficiently clear to require that the SNS remove the PII of a registered user only when they are informed of the location. Rather, it could be read to

require the request for removal of PII to state any known location, but if the requestor did not know the location, leave it up to the SNS to find the information.

d) There is no deterrent for persons who would maliciously request a SNS to remove the PII of another person in the bill, therefore potentially subjecting a SNS to liability from a claim brought by persons whose PII was stricken from their site based upon a fraudulent request.

e) Recent amendment language which added 65(b), contains imprecise language referring to "unintentional violations" of the provisions of the bill, and could create a loophole by giving a defense for any claim that the respondent unintentionally violated the law, which is a different standard than the "willful and knowing" standard for liability in subsection 65(a). In addition, "unintentional violation" does not have a legal meaning, and thus would necessitate litigation to clarify its meaning.

f) There are situations where a person may violate the provisions of the bill through attempting to follow its mandates. I.e. Section 60(a) requires information be removed "in a timely manner" upon request; (b) requires sufficient information to verify the identity of a registered user; while 62(a) defines "timely manner" to mean within 96 hours. It is easily conceivable that a request may come in to a SNS to remove PII without sufficient identifying information. Were the SNS to request further information sufficient to verify the request is valid in compliance with 60(b), the time for compliance under 60(a) might toll before the SNS could comply with the request - thereby exposing them to liability.

7) Related Pending Legislation:

a) AB 1291 (Lowenthal), would create the Right to Know act of 2013, repealing and reorganizing certain provisions of existing law pertaining to the disclosure of a consumer's personal information. Status: Assembly Judiciary Committee.

b) SB 568 (Steinberg), would prohibit an operator of an Internet Web site, online service, online application, or mobile application, from marketing or advertising a product or service to a minor if the minor cannot legally purchase the product or participate in the service in the State of California. This bill would also prohibit an operator from using, disclosing, or compiling, or allowing a third party to knowingly use, disclose, or compile, the personal information of a minor for the purpose of marketing goods or services that minors cannot legally purchase or engage in the State of California. Status: Currently pending before this Committee.

8) Related Prior Legislation:

a) ACR 106 (Nava) of the 2007-08 Legislative Session, would have urged user-generated content Web sites to work with the Safety Technical Task Force and law enforcement to reduce the use of those Web sites for purposes of criminal behavior. ACR 106 died on the Assembly Inactive File.

b) AB 632 (Davis) of the 2009-10 Legislative Session, would have required a social networking Internet Web site to provide a disclosure to users that an image which is uploaded onto the Web site is capable of being copied, without consent, by persons who

view the image, or copied in violation of the privacy policy, terms of use, or other policy of the site. AB 632 was vetoed.

c) SB 1361 (Corbett) of the 2009-10 Legislative Session, would have prohibited a social networking Internet Web site, as defined, from displaying, to the public or other registered users, the home address or telephone number of a registered user of that Internet Web site who is under 18 years of age, as provided. SB 1361 failed passage in this committee.

d) SB 242 (Corbett) of the 2011-12 Legislative Session, would have prohibited a social networking Internet Web site from displaying the home address or telephone number, in specified text fields, of a registered user who identifies himself or herself as under 18 years of age. SB 242 failed passage on the Senate Floor.

e) SB 761 (Lowenthal) of the 2011-12 Legislative Session, would have required the Attorney General, by July 1, 2012, to adopt regulations that would require online businesses to provide California consumers with a method for the consumer to opt out of the collection or use of his or her information by the business. SB 761 was returned to the Secretary of the Senate by the Senate Appropriations Committee pursuant to Joint Rule 56.

REGISTERED SUPPORT / OPPOSITION:

Support:

Alameda County District Attorney's Office
Alameda County Sheriff's Office
California Partnership to End Domestic Violence
California State Parent Teachers Association
California State Sheriff's Association
Child Abuse Prevention Center
Common Sense Media
Crime Victims United of California
Klass Kids Foundation
Los Angeles County Sheriff's Department
Peace Officers Research Association of California

Opposition:

Association for Competitive Technology
American Civil Liberties Union of California
America Online Inc.
Application Developers Alliance
Bay Area Council
CalChamber
California Hispanic Chambers of Commerce
Center for Democracy & Technology
Computer & Communications Industry Association
Electronic Frontier Foundation

Engine
Facebook
Family Online Safety Institute
Google
iKeepSafe
Internet Alliance
LGBT Technology Partnership
LinkedIn
MapQuest
Motion Picture Association of America
Moviefone
NetChoice
Patch
Silicon Valley Leadership Group
State Privacy and Security Coalition, Inc.
Stop Child Predators
TechAmerica
TechNet
The Huffington Post
The Internet Association
Tumblr
WiredSafety
Zynga

Analysis Prepared by: Dana Mitchell / A.,E.,S.,T. & I.M. / (916) 319-3450