Industry Opposition Letter Gets It Wrong:
Here's How the Right to Know Act (AB 1291) Actually Works

On March 26, 2013, several industry groups sent an opposition letter about the California Right to Know Act (AB 1291) to the bill's author, Assemblymember Bonnie Lowenthal. This letter contained several inaccuracies and misunderstandings related to the bill language. This document sets the record straight.

The California Right to Know Act (AB 1291) is supported by a diverse coalition of the state's leading domestic violence advocates, women's groups, sexual health organizations, and civil liberties and consumer privacy groups: ACLU of California, California NOW, California Partnership to End Domestic Violence, California Public Interest Research Group (CalPIRG), Consumer Action, Consumer Federation of California, Consumer Watchdog, Electronic Frontier Foundation, Internet Sexuality Information Services, Privacy Activism, Privacy Rights Clearinghouse, Privacy Times, and World Privacy Forum.

Industry says:

> While we understand that the bill is sponsored by several consumer organizations, it is unworkable, rests on mistaken assumptions about how the Internet works, and would impose costly and unrealistic mandates on California's technology sector with minimal benefit to state residents.

Fact: The way the Internet "works" today is that companies are collecting and disclosing vast amounts of Californians' sensitive personal information to third parties - including online advertisers, data brokers, and third party apps - in ways that Californians do not realize and could cause them harm.

- Websites incorporate up to 100 tracking tools that collect very personal information like age, gender, race, income, health concerns and recent purchases for third party advertising and marketing companies when consumers visit webpages.[1] Profiles of personal information are bought and sold on stock-market-like exchanges.[2]
- Third party data broker companies buy, sell, and trade personal information obtained from mobile phones, financial institutions, social media sites, and other online and brick and mortar companies.[3]
- Many mobile applications are sharing personal information, such as location information, unique phone identification numbers, and age, gender, and other personal details of both adults and children with third party companies.[4] Several women and children have been hurt or killed when cell providers or applications collected and then shared location data with abusers.[5]
- Facebook apps used by a consumer's "friends" can often access sensitive information about that consumer, including religious, political, and sexual preferences.[6]
- Companies tracking and collecting information about purchases and activities, online and off, are using it in ways people do not expect or want. Target revealed a woman's pregnancy before she told her family.[7] Americans have lost jobs[8] and been denied mortgages[9] when data brokers shared incorrect information and scammers use data broker lists to target vulnerable populations like seniors.[10]

Fact: AB 1291 modernizes California's current transparency law[11] that has been in place for a decade and mirrors existing European Union data access rights.

Fact: The White House,[12] the Federal Trade Commission,[13] and the California Attorney General[14] all support data transparency and access for consumers.

Fact: AB 1291 will modernize current transparency law to make it work more effectively, efficiently, and minimize costs.

- Unlike many other privacy laws, AB 1291 does not require costly affirmative notice to Californians about personal information that is retained or disclosed, but only requires companies to respond to Californians who make requests. Requests are limited to one per 12-month period.
- The bill takes advantage of the past decade's technological advances and provides new flexibility in the means available to businesses to communicate with Californians. Companies may utilize an automated portal or other mechanisms already in place to provide access to data required by European law or choose to provide "just in time" notice to Californians about personal information disclosed rather than responding to requests.
- Better transparency has also proven to be good for business and the bottom line. Mandatory data breach notification laws in 45 states and the resulting improvements in data protection saved companies an average of $19 million in 2011.[15]

Fact: Californians want the right to know what is happening to their personal information.

- 82% of registered California voters – across demographic, regional and political spectrums – are concerned about how their personal information is being collected by Internet and mobile companies.[16]
- 69% of Americans believe there should be a law that gives people the Right to Know everything a website knows about them.[17]

Industry says:

AB 1291 is over-broad. It would expand the definition of "personal information" under California's Shine the Light Law to cover not only any information that identifies "or references" an individual, but also any information that identifies or "is able to be uniquely associated with a particular device". It would specifically reach IP addresses and device identifiers, as well as information that could be associated with that information.

Fact: AB 1291's definition of personal information is now consistent with current California law and federal privacy recommendations and incentivizes privacy-protective steps.

- AB 1291's definition of personal information modernizes the existing law's under-inclusive definition that fails to properly cover sensitive personal information such as location information and sexual orientation. The modernized definition now makes it consistent with current California law and the Federal Trade Commission's 2012 privacy guidelines, which cover all information that can be "reasonably linked" to a consumer, and ensures that Californians will know when their sensitive personal information is retained or disclosed.
- Because the definition of personal information does not include information that cannot be associated with a particular individual or device, a company's compliance burden is commensurate with the amount of personal information that it retains. Companies that disassociate or aggregate information prior to retention or disclosure are not subject to AB 1291.

Industry says:

Although the bill says that it applies to "customers", in fact AB 1291 would apply to any California resident who "with or without an exchange of consideration" provides any of a wide sweeping range of non-personally identifying information to a business. This means the bill would reach every website or other

Fact: AB 1291 applies to relationships without an exchange of consideration because "free" services retain and disclose extensive information about consumers.

- AB 1291 retains the language from current law that enables a Californian to use the law to learn regardless of whether the relationship is "with or without an exchange of consideration."[18] This is all the more important today to ensure that Californian customers can use the Right to Know law to learn how their personal information has been retained or disclosed whether companies have a business model of monetary payment or make their money from selling or sharing a customer's personal information with online advertisers, data brokers, or other third parties.

Fact: AB 1291 does not apply when a business does not retain or disclose personal information about a California resident.

- AB 1291 empowers California residents to learn how a business has retained or disclosed their personal information. It applies only to businesses that retain or disclose such information. A business that retains or discloses only non-personal information (or no information at all) is not subject to AB 1291's provisions.

Industry says:

> It would require any business that runs a computer server and receives this information to do three expensive and unworkable things without any ability to defray the costs of this mandate.

Fact: AB 1291 gives Californians access to data rights that Europeans already have and that have proved workable for many years

- Many companies already comply with existing European privacy laws and have built the infrastructure and any necessary verification processes to provide access to personal information.
- Many companies already provide mechanisms for consumers to view their own information. Facebook[19] and Google[20] already provide automated access to personal information for Americans as well as Europeans.[21]

Industry says:

> First, businesses would need to provide "to the 'customer' free of charge, access to, or copies of", all of the amorphous range of information about the "customer" stored by the business. The information would need to be provided in a personalized or standardized format. This mandate is unworkable for the following reason. Businesses would not be able to authenticate customers on the basis of an IP address or device identifier because both numbers relate to a router or a device, not an individual.

Fact: AB 1291 only requires disclosure of specific customer information when a business can "reasonably authenticate" that the person seeking the information is the customer.

- The bill also only requires a specific response to a customer when this information is reasonably available, it continues the current law's requirement that companies are only required to respond to customers with the categories of personal information disclosed, and overall compliance costs are commensurate with the amount of personal information that a company has not taken the privacy protective step of de-identifying before retention or disclosure.

Second, businesses would have to provide the name and address of each entity to whom the information is disclosed – even if they have no idea of the name or address. It is important to recognize that servers on the Internet will sometimes automatically forward along the IP address or device identifier number of a "host" that connects to the server in the course of forwarding a request or communication from the "host" along to its destination. Recall that no payment need occur. A California user would simply need to send a communication through the Internet to impose this obligation on every business whose server handles the communication.

Fact: AB 1291 does not require a business to provide specific information that is not "reasonably available" to the business.

- Internet service providers and other businesses that do not retain records about routing communications are not required to do so in order to comply with the law.
- Any business that disassociates or aggregates its logs is not subject to the burden of complying with the law.

Fact: AB 1291 only requires disclosure of specific customer information when a business can "reasonably authenticate" that the person seeking the information is the customer.

Industry says:

Third, the bill would go even farther, requiring notice "prior to or immediately after the disclosure" regardless of whether the "customer" had requested the disclosure. Californians would be deluged with disclosures each time an IP address, device identifier, or other information on the bill's very long list of personal information was disclosed automatically or through a conscious decision by the business.

Fact: This is inaccurate. AB 1291 actually provides companies with new flexibility to choose between responding to a customer-initiated request OR providing information proactively with a "just-in-time" notice prior to or immediately after a disclosure.[22]

Industry says:

Furthermore, this bill would reopen the door to unfair competition lawsuits. Proposition 64 was supported by the business community and passed by the voters with overwhelming support in order to help protect California's businesses from shakedown lawsuits brought under the unfair competition law. AB 1291 would undermine such limitations. It not only imposes unworkably broad new regulations, it would then allow a lawsuit for any technical violation. This is a recipe for abusive and costly lawsuits that may benefit the trial bar, but harm businesses operating in California.

Fact: This is incorrect. AB 1291 maintains the same penalty provisions as current California law and also continues to give companies a lengthy 90-day cure period to fix any violations.[23]

---

[1] Julia Angwin, *The Web's New Goldmine: Your Secrets*, Wall St. J., July 30, 2010, *available at* http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html; *see also* Charles Duhigg, *How Companies Learn Your Secrets*, NY Times, Feb. 16, 2012, at MM30, available at: http://goo.gl/ayHjN (discussing how one retail businesses' collection and sharing of information revealed a teenager's pregnancy before her family knew); Geoffrey A. Fowler, *When the Most Personal Secrets Get Outed on Facebook*, Wall. St. J., Oct. 13, 2012, available at http://goo.gl/iwG0i (discussing how the default privacy settings of a LGBT Facebook outed the sexual orientation of two college students who were added to the group).

[2] http://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-by-advertisers.html?smid=tw-share

[3] Natasha Singer, *Congress to Examine Data Sellers*, NY Times, Jul. 25, 2012, at B1, *available at* http://www.nytimes.com/2012/07/25/technology/congress-opens-inquiry-into-data-brokers.html?_r=0.

[4] Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, Wall St. J., Dec. 17, 2010, available at: http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html; *see also* Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL. ST. J., Aug. 4, 2010, available at: http://goo.gl/sCFTz (discussing how Women and children have been hurt or killed when cell providers or applications have shared location data with abusers).

[5] Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL. ST. J., Aug. 4, 2010, available at: http://goo.gl/sCFTz.

[6] Julia Angwin & Jeremy Singer-Vine, *Selling You on Facebook*, Wall. St. J., Apr. 7, 2012, available at: http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html?mod=WSJ_WhatTheyKnowPrivacy_LeftTopNews.

[7] Charles Duhigg, *How Companies Learn Your Secrets*, NY Times, Feb. 16, 2012, at MM30, available at: http://goo.gl/ayHjN.
[8] http://finance.yahoo.com/news/ap-impact-criminal-past-isnt-182335059.html
[9] http://money.msn.com/credit-rating/denied-credit-maybe-youre-dead
[10] http://www.nytimes.com/2007/05/20/business/20tele.html?_r=0
[11] http://codes.lp.findlaw.com/cacode/CIV/5/d3/4/1.81/s1798.83
[12] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
[13] http://ftc.gov/os/2012/03/120326privacyreport.pdf
[14] http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-issues-guidance-how-mobile-apps-can-better
[15] 2011 Cost of Data Breach Study: United States, Ponemon Institute, Mar. 2012, http://goo.gl/qeyUG.
[16] Voters Across the Political Spectrum Concerned About Tech Companies Invading Their Privacy, Press Release, Mar. 31, 2012, USC Dornsife/Los Angeles Times, available at http://dornsife.usc.edu/usc-lat-poll-privacy-march 2012/.
[17] Joseph Turow et al., Americans Reject Tailored Advertising and the Three Activities that Enable It (Sept. 2009), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.
[18] Civ. Code 1798.83(e)(5).
[19] *Accessing Your Facebook Info*, Facebook.com, http://en-gb.facebook.com/help/405183566203254 (discussing how consumers can access their "Expanded Archive").
[20] *Google Takeaway*, Google UK, http://goo.gl/SOEZj.
[21] Council Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT.
[22] Proposed 1798.83(b)(1)-(2).
[23] Cal. Civil Code §1798.84.