

# LOSING THE SPOTLIGHT

## A STUDY OF CALIFORNIA'S SHINE THE LIGHT LAW

Gained a  
few pounds

Shopped for wedding rings

I voted for her

Went to gay  
pride parade

Bought  
pregnancy test

Still email my ex-boyfriend

Searching for new job

**S**unlight is said to be the “best of disinfectants.” And transparency plays an essential role in both incentivizing companies to better protect consumer privacy and empowering consumers to make privacy-protective choices.

That’s why the landmark Shine the Light law (Cal. Civil Code § 1798.83) was intended to give Californians the right to know the “who, what, where and when” of how a business handles personal information. Californians should be able to use this important transparency law, passed in 2003, to learn what’s happening to their personal information.

But fast forward a decade: exponential advances in technology as well as drastic changes in business practices have outpaced current law. Every day, millions of Californians now search and shop online, connect via social networking, or use a mobile device, leaving behind a vast trail of personal information in the form of search and chat histories, buying habits, photos, friend lists, and more. Consumers are increasingly in the dark about how information on where they go, who they know, and what they do is being collected and shared with data brokers, online advertisers, and third party apps — and even the government.

The ramifications of personal information being collected and shared in ways that consumers do not intend or desire range from embarrassing to downright dangerous. So it is not surprising that an overwhelming majority of Californians—from across the political and demographic spectrum—are concerned about companies collecting their personal information, and most Americans think there should be a law giving them the right to know everything a website knows about them.

As the Shine the Light law turns a decade old, it is a good time to examine this important transparency law and draw specific lessons that can inform state, national, and international policymakers and businesses seeking to protect privacy and increase transparency about data collection, use, and sharing in the modern digital era.

Part I of this policy paper provides background on why transparency measures such as Shine the Light play an essential role in safeguarding privacy. Part II evaluates the current law’s effectiveness and identifies loopholes and limitations in its use and implementation. Part III discusses increased attention on transparency by state, federal and international policymakers and the business community. Finally, Part IV suggests policy principles for updating California privacy law and better informing consumers about how their personal information is collected and shared.

For more information and resources about California’s Shine the Light law and policy efforts related to increasing transparency about how personal information is collected and shared, visit [www.aclunc.org/r2k](http://www.aclunc.org/r2k). You can also contact us directly with questions or comments at [dotrights@aclunc.org](mailto:dotrights@aclunc.org).

# TABLE OF CONTENTS

<b>INTRODUCTION.....</b>	<b>1</b>
<b>PART I: Why Is Transparency So Important Today? .....</b>	<b>2</b>
<b>PART II: Is Shine the Light Giving Consumers Transparency? .....</b>	<b>9</b>
<b>PART III: Consumer Transparency Measures Enjoy State, National, and International Support.....</b>	<b>13</b>
<b>PART IV: A Common-Sense Update for Shine the Light.....</b>	<b>17</b>
 Give Consumers the Right to Learn What Personal Information Companies Collect and Disclose about Them.....	<b>17</b>
 Provide Transparency for All Modern Information Collection and Disclosure.....	<b>17</b>
 Have Simple and Efficient Request and Response Requirements.....	<b>18</b>
 Make Sure Transparency Law is Consistent with Legitimate Business Practices and Can Be Fairly Enforced.....	<b>19</b>
<b>CONCLUSION.....</b>	<b>19</b>

CONTRIBUTING WRITERS: Nicole A. Ozer and Matt Cagle, Technology and Civil Liberties Project, ACLU of Northern California

DESIGN: Anna Salem, ACLU of Northern California

COVER: Gigi Pandian, ACLU of Northern California

PRINTING: Inkworks Press  [INKWORKSPRESS.ORG](http://INKWORKSPRESS.ORG)

Published by the ACLU of California, November 2013

*This publication is supported by cy pres funds and the generosity of the ACLU's members and donors.*

# INTRODUCTION

The Shine the Light law was intended to provide California consumers with the right to know the “who, what, where, and when” of how a business handles personal information.”<sup>1</sup> This important transparency law gave Californians the right to learn how companies share their personal information with third parties for “direct marketing purposes”—solicitation by postal mail, telephone, or email.<sup>2</sup> The law empowered Californians and incentivized companies to take privacy-protective steps.

Shine the Light was a landmark law when it was passed in 2003. But fast forward a decade. Technology has advanced exponentially, business practices have changed dramatically, and consumers have started to live truly digital lives. Every day, millions of Californians search online, shop, or use a mobile device, leaving behind a vast trail of personal information in the form of search and chat histories, photos, friend lists, and more. Many companies are collecting and sharing these detailed digital footprints about who we are, where we go, what we do, and who we know with online advertisers, third party applications, data brokers, and even the government.

As a result, Californians are very concerned about threats to their personal privacy. Eighty-two percent of Californians—from across the political and demographic spectrum—are concerned about companies collecting their personal information.<sup>3</sup> Sixty-nine percent of Americans believe there should be a law giving them the right to know everything a website knows about them.<sup>4</sup> Consumers are right to be concerned and to want to know more.

But the data-sharing practices that the Shine the Light law was designed to address have been eclipsed by technological developments. Targeted advertising, data brokers, third party applications, and other technologies have vastly increased the potential for personal information to be collected and shared in ways that individuals do not expect or want. As a result, they pose new threats to privacy that Shine the Light did not anticipate.

As Shine the Light turns a decade old and state, national, and international policymakers increasingly discuss the importance of consumer transparency, it is a good time to examine this important law. Is the law bolstering and supporting the inalienable right to privacy of all Californians?<sup>5</sup> Is it adequately providing consumers with transparency and the useful information they need? What works and what does not work in practice? And what policy steps might be necessary to ensure that consumer transparency rights work effectively in the modern digital era?

This policy brief examines the current state of corporate transparency via the Shine the Light law. Part I explains why transparency measures such as Shine the Light are essential. Part II evaluates the law’s effectiveness. Part III considers recent political and business support for increased consumer transparency and how these advances inform policy arguments. Finally, Part IV suggests some policy principles for updating privacy laws and better informing consumers about how their personal information is collected and shared.

# PART I: Why Is Transparency So Important Today?

The need for robust transparency rights is even more marked today than it was 10 years ago when Shine the Light became law. Advances in technology now enable businesses, both online and offline, to collect vast amounts of personal information in sophisticated ways, retain it indefinitely, and share it quickly with others, including advertisers, data brokers, third party applications, and the government. Although recent studies show increased public concern about the privacy of personal information, consumers understand very little about the technologies and privacy policies that govern the information itself.<sup>6</sup> When transparency requirements reveal how personal information is treated, consumers make more privacy-protective choices and companies are incentivized to adopt privacy protective practices.

## Californians Are Concerned about How Their Personal Information Is Collected and Shared

Eighty-two percent of Californians—across the political and demographic spectrum—are concerned about companies collecting their personal information.<sup>7</sup> Seventy-eight percent of California voters—including 71 percent of voters age 18-29—also say the collection of personal information online is an invasion of privacy.<sup>8</sup> This widespread concern is echoed both nationwide and across the world. As of 2010, nearly eight in 10 global consumers, consistent across age groups and regions, expressed concern about unauthorized access to their personal information—a 6 to 8 percent increase since 2008.<sup>9</sup> By 2011, privacy rose to the top of the list of concerns for many mobile users,<sup>10</sup> and 58 percent of social network users were concerned about privacy.<sup>11</sup> All in all, 68 percent of Internet users believe current laws do not adequately protect people's privacy online,<sup>12</sup> and 69 percent of Americans believe there should be a law giving them the right to know everything a website knows about them.<sup>13</sup>

**82 percent of Californians—  
across the political and  
demographic spectrum—  
are concerned about  
companies collecting their  
personal information.**

**—USC/Los Angeles Times Poll**

## Californians Do Not Know How Companies Collect and Share Their Information

Californians have very little understanding about how companies are actually collecting and sharing their personal information. A 2010 study posed five true/false questions about online privacy, and 75 percent of online adults answered two or fewer of these questions correctly.<sup>14</sup> Of that group, 48 percent incorrectly believed their consent is required for companies to use the personal information they collect from online activities.<sup>15</sup> An earlier survey revealed that almost half of Californians wrongly believe that privacy policies prohibit businesses from sharing information and more than half think that privacy policies require companies to obtain a user's consent before selling their personal information.<sup>16</sup> A 2012 study further revealed that only 38 percent of Internet users are generally aware of ways they can limit how much of their information is collected by a website.<sup>17</sup>

It is not surprising that consumers do not understand corporate information practices. It would take the average consumer up to 293 hours per year just to skim the privacy policy at each website they visited and up to 304 hours to

actually read them.<sup>18</sup> In the wake of privacy roundtables held by the Federal Trade Commission, the agency noted that “consumers generally lack full understanding of the nature and extent of [data collected by third parties].”<sup>19</sup> Largely invisible data collection practices and long and confusing privacy policies were cited as contributing factors to this problem.<sup>20</sup> Company leaders have also admitted that the technology industry has not done enough to educate consumers about how products and services work and their impact on consumer privacy. In 2011, Steve Jobs, the late co-founder, chairman, and CEO of Apple, told an interviewer, “As new technology comes into the society there is a period of adjustment and education. We haven’t—as an industry—done a very good job educating people, I think, as to some of the more subtle things going on here.”<sup>21</sup>

## Knowing How Personal Information Is Collected and Shared Sparks Changes in Consumer Behavior and Business Practices

Transparency is the spark that empowers consumers to make privacy-protective choices and incentivizes companies to take privacy-protective actions on consumers’ behalf. Consumers make more privacy-protective choices when they know how their personal information is collected and shared. In a July 2013 study, 62 percent of respondents said they would be “not likely at all” to repeat a purchase from a company that shared their personal information with a data broker, and 37 percent of the same group said they had abandoned an online transaction due to something they learned about by reading a company’s terms of service.<sup>22</sup> In a 2009 study, 66 percent of Americans said they did not want marketers to tailor advertisements to their interests, and the respondents’ rejection of targeted advertising rose to 84 percent after they were told about common methods of data collection.<sup>23</sup> Analysis of the impact of data breach notification laws in California and around the country also reveal that when consumers learn about a data breach, they are enabled to take specific actions to increase their level of care and mitigate loss.<sup>24</sup>

**54 percent of smartphone users have decided not to download an application after learning how much personal information it wanted to access.**

**—Pew Research Center**

Consumers also make more privacy-protective choices on their mobile devices when they know how their personal information is collected or shared. Fifty-four percent of smartphone users have decided not to download an application upon discovering how much personal information they would need to share to use it, and 30 percent have uninstalled an application upon learning it collected more personal information than they wanted to share.<sup>25</sup> In total, 57 percent of app users have taken a privacy-protective action after learning about how their personal information would be shared.<sup>26</sup>

**The passage of the California Shine the Light law in 2003 prompted 69 percent of surveyed companies to tighten information sharing practices and controls with marketers.**

**— Ponemon Institute**

Consumers also prefer websites and services that they know collect and share their personal information responsibly.<sup>27</sup> Sixty percent of online shoppers are influenced to visit websites and make purchases based on how companies handle personal information.<sup>28</sup> Researchers have also found that individuals with more access to information about the privacy practices of companies chose to purchase from merchants that offer more privacy protection and were willing to pay a premium to purchase from such merchants.<sup>29</sup> The researchers concluded that “once people were provided with salient privacy

information, they chose sites they considered privacy protective.”<sup>30</sup> A consumer with actual information—and not just vague promises—about how a company handles her personal information is more able to evaluate whether to trust and stick with a company.<sup>31</sup> Behavioral research also suggests that providing specific information with personal relevance to an individual can be more effective than a general disclosure and increase the likelihood that a person will take action.<sup>32</sup>

Transparency requirements also incentivize companies to better protect consumer privacy. The passage of the original Shine the Light law prompted 69 percent of companies surveyed to “tighten information-sharing practices and controls with marketers,” and 56 percent said they would limit information-sharing with direct marketers.<sup>33</sup> Forty-four percent of respondents said they had implemented (or planned to implement) stronger due diligence procedures before sharing customer information with third parties.

A host of scholars have demonstrated the profound effect of transparency regarding information practices on future behavior. One example is data breach notification laws, first passed in California in 2002 and now adopted in some form by 45 other states and the District of Columbia.<sup>34</sup> These laws require that companies provide consumers with information about breaches of their information in a timely manner. Data breach laws have influenced corporate steps to better protect consumer privacy, including the development of stronger data security structures to prevent breaches, the increased importance of privacy staff, and the encryption of personal information.<sup>35</sup> In California, 50 percent of companies reporting breaches in 2012 also offered additional services to consumers to help offset harm, including the opportunity to subscribe to credit monitoring or a similar “identity theft protection” product, even though these actions were not required by the law.<sup>36</sup> All in all, from 2002 to 2009, data breach laws helped to reduce identity theft on average 6.1 percent and saved American consumers nearly \$93 million per year, all the while “paying off” for companies with reduced losses due to data breaches.<sup>37</sup>

Financial transparency law has also led companies to take privacy protective actions that empower consumers. Under the federal Gramm-Leach Bliley Act (GLB), for instance, financial institutions must provide customers with a notice about their information collection and information-sharing practices and allow them the ability to opt out of certain forms of sharing.<sup>38</sup> These transparency requirements have been found to trigger positive behavior in companies including the inspection of their own practices, often for the first time, to learn just how data is and is not shared, and the creation of a “detailed roadmap for privacy compliance ... all of which benefit consumers.”<sup>39</sup>

**Transparency will “empower consumers to make sure they are being treated fairly.”**

**—FTC Chairwoman Edith Ramirez**

In 1914, U.S. Supreme Court Justice Louis Brandeis famously observed that “[s]unlight is said to be the best of disinfectants.”<sup>40</sup> Almost 100 years later, Federal Trade Commission Chairwoman Edith Ramirez echoed this sentiment, emphasizing the “need to move commercial data practices into the sunlight” and calling “transparency ... an essential part of the solution” to current issues of information privacy.<sup>41</sup> According to Ramirez, transparency “will empower consumers to make sure that they are being treated fairly.”<sup>42</sup> Brandeis’s and Ramirez’s comments highlight how even as technology has advanced in recent decades, the crucial role of transparency in protecting privacy has not. As Americans rely more and more on technology to improve their lives, they should know what information is being collected and with whom that information is being shared.

# Consumers Are in the Dark about Modern Information Collection and Sharing

Dramatic changes in technology and business practices mean that personal information is being collected from consumers in many new ways. Data brokers, third party advertisers, and apps are key drivers in the consumer data business today and yet consumers find it exceedingly difficult to learn how these businesses collect and share their personal information.

## Data Brokers

Data brokers are businesses that buy, sell, and trade personal information obtained from both public records and private sources, including mobile phones, financial institutions, social media sites, and online and brick and mortar companies.<sup>45</sup> These companies have amassed an enormous repository of information about a wide range of activities that includes data about almost every adult American. For example, Acxiom, the “big daddy of data brokers,” holds records on a majority of adults in the United States, and Datalogix has information on almost every American household, including on more than \$1 trillion in consumer transactions.<sup>46</sup> And these brokers collect not only commercial and financial information but also information about people’s communications, social connections, and more. Ropleaf advertises having “Real-time data on 80 percent of U.S. emails”<sup>47</sup> and PeekYou analyzes “content from over 60 social sites, news sources, homepages and blog platforms and identifies the actual people behind it, combining their scattered digital footprints into a comprehensive record of their online identity.”<sup>48</sup>

**Data Brokers Link Purchase History to Facebook Users.** Using loyalty card and payment tracking programs to create profiles based on purchase history and habits is big business. Last year, Facebook announced a partnership with data broker Datalogix that involves comparing batches of Facebook users shown an ad for a specific product with Datalogix’s consumer purchase records for the same users.<sup>43</sup> In February 2013, Facebook announced that it will expand the linking of offline and online data, allowing marketers to target users with data acquired from data brokers.<sup>44</sup>

Utilizing large-scale data mining operations, data brokers organize the available information into lists with specific characteristics that other companies or entities would like to buy to target particular individuals. Information organized by these data brokers may be sought out by online services, advertisers, and even the government. Some purchasers use the information to create targeted advertising based on the brokers’ specific classification of that individual.<sup>49</sup> For example, data brokers sell third parties raw data and lists of profiles grouped by vice or vulnerability with labels such as “Gaming-Casino,” “dieters,” or “Suffering seniors.”<sup>50</sup> Others combine information about consumers’ online activity with information brokers collect about purchases at brick and mortar stores or from loyalty card programs.<sup>51</sup>

With the detailed dossiers data brokers hold on most Americans, it’s no surprise commercial enterprises may want to use the data to make decisions about the services they provide—but other actors we rely on for services are also purchasing and using data acquired from brokers. In 2012, the *Wall Street Journal* reported that a North Carolina-based health insurance company bought data broker information for 3 million people in its employer group plans.<sup>52</sup> Even the U.S. government is a customer—with agencies like the FBI circumventing federal Privacy Act safeguards<sup>53</sup> intended to limit

government data collection, by just tapping these massive databases when they want information about an individual.<sup>54</sup> Unfortunately, despite the expanding markets for data, data brokers themselves have “operated in the shadows for years” and continue to offer consumers very limited access to their industry vaults.<sup>55</sup>

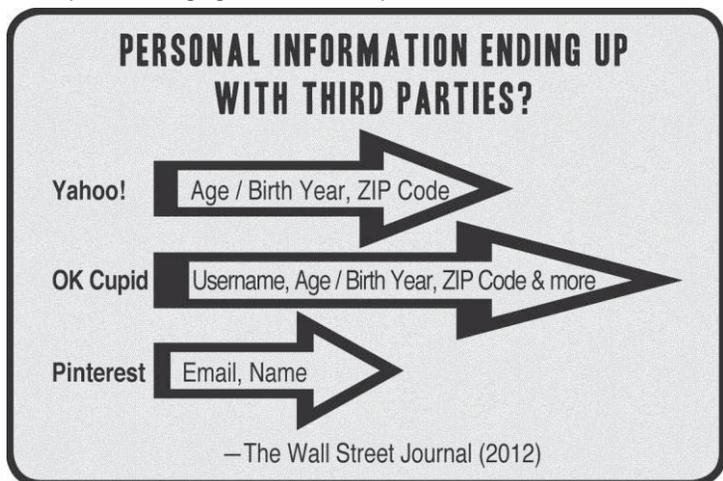
FTC Commissioner Julie Brill has noted that “even well-educated consumers have had difficulty obtaining meaningful information about what the data brokers know about them” and “that current access and correction rights provide only the illusion of transparency.”<sup>56</sup> Without transparency into how data brokers buy and sell detailed personal profiles of consumers every day, it is impossible to know the true privacy impact of these activities. Still, it is known that data broker mistakes and disclosures contribute to a variety of real-life harms including fraud, lost jobs, and denied credit. In one case, a scammer used a data broker list to call a 92-year-old Army veteran, obtain his banking information, and steal \$100,000 of his retirement savings.<sup>57</sup> A Massachusetts woman who was denied a job discovered that the commercial background check company the employer used had improperly linked her to a criminal indictment.<sup>58</sup> Another couple’s credit was ruined due to an incorrect mortgage default notation shared by a data broker.<sup>59</sup> In 2012, the FTC levied an \$800,000 fine against Spokeo, a company involved in providing information for background checks, for failing to ensure the accuracy of its profiles, which can include postal and email addresses, phone numbers, age and marital status, hobbies, ethnicity, religion, photos, and activities on social media sites.<sup>60</sup>

## Targeted Advertising

Since the passage of Shine the Light, the use of online advertising has grown, especially targeted advertising. Targeted advertising is capable of serving different ads to different recipients who visit the same web page or use the same app based on information about that recipient. While some forms of targeted advertising operate without collecting and retaining information at all, others rely on building detailed profiles about individual consumers in order to determine which ad to deliver.

There are two ways that targeted advertisers obtain information about individuals. First, they may receive information directly, either from the individual herself (though she may not be aware that the information will be used for advertising purposes<sup>61</sup>) or from other companies. For example, a 2012 study of 70 popular websites found that many share a user’s real name, email address, or other identifying information (such as a username) with third-party companies.<sup>62</sup> Other companies engage in a technique called behavioral advertising that relies on building up a comprehensive record of an

individual’s online activities in order to determine her characteristics and interests. Behavioral advertising companies frequently use methods such as web cookies to record as much information as possible about an individual’s online activities.<sup>63</sup> This web tracking requires the cooperation of the web site that the consumer is trying to visit; some sites install trackers from up to 100 different companies that allow those third parties to record activity on the site.<sup>64</sup>



The information collected from consumers online is also combined with other data-mining operations to add even more value to targeted advertisements. Companies combine information from in-store purchases, mobile devices, financial institutions, and social media sites into huge “behavioral databanks” for use in targeting these ads.<sup>65</sup> As smartphone usage expands, companies are engineering new ways to link devices to a single user who can then be profiled and targeted with ads.<sup>66</sup> Targeted ads typically sell for twice as much as generic ads because they are twice as effective.<sup>67</sup> More and more, companies sell opportunities to display these targeted ads on markets resembling stock exchanges,<sup>68</sup> a growing market expected to rise further to \$8.3 billion by 2017.<sup>69</sup> This “[b]usiness of spying on consumers” is “[o]ne of the fastest-growing businesses on the Internet.”<sup>70</sup>

**“One of the fastest-growing businesses on the Internet... is the business of spying on Internet users.”**

**—The Wall Street Journal**

The majority of consumers polled in numerous national surveys have consistently expressed concern with behavioral targeting, with 68 percent in a 2012 Pew poll agreeing with the statement that they were “NOT OKAY with targeting advertising because I don’t like having my online behavior tracked and analyzed.”<sup>71</sup> A 2009 academic study found that 66 percent of adult Americans do not want marketers to tailor online advertisements to their interests.<sup>72</sup> Consumers have expressed particularly marked concern with advertising that integrates online and offline activities—86 percent do not want websites to show them advertisements tailored to them based on their offline activities.<sup>73</sup>

Consumers are right to be concerned. The information-crunching process behind the delivery of targeted ads can reveal very private information, both accurate and inaccurate. Data tracking and targeting programs have revealed important—and sensitive—information about a pregnancy,<sup>74</sup> incorrectly labeled someone as having a medical condition,<sup>75</sup> and resulted in discriminatory marketing of products.<sup>76</sup>

**Target tracks purchases, “targets” ads, and reveals a woman’s pregnancy**—Retailer Target keeps such close track of the purchase patterns of its shoppers that it revealed a woman’s pregnancy to her family by sending coupons for baby items to her home address before she announced the news.<sup>77</sup>

**Marketers target ads based on inferences about health condition.** When an invitation to join a support network for multiple sclerosis patients arrived in the mail, the woman that received it was surprised—she did not have the disease.<sup>78</sup> An investigative reporter followed the “winding path” leading to that invitation and tracked the false information back through a marketing company to discover that the inference originated due to an online survey the woman had filled out years before.<sup>79</sup> Without transparency about disclosure practices, this woman and many other Americans are most often left in the dark about when and how true or false information about their health is ending up in the hands of third parties and how it might be used.

**Companies offer different options or charge different prices based on who you are**—Travel website Orbitz was exposed in 2012 for showing consumers different hotels in different price brackets based on their location and type of computer.<sup>80</sup> In 2013, major airlines also announced a policy change that will enable them to begin profiling consumers and to charge different people different prices as well.<sup>81</sup> This practice of “Weblining”—denying people opportunities based on their digital selves<sup>82</sup>—could continue to grow and lead to harms similar to the decades-old practice of “redlining,” where banks and financial institutions denied services based on race or residence in inner city neighborhoods.<sup>83</sup>

## Third Party Applications

Consumers are increasingly using small software applications, or “apps,” within social networking services and on smart phones and other connected devices.<sup>84</sup> Apps may have access to a wide variety of sensitive personal information on a device or service, including location, unique phone or device identifiers, and personal details such as age and gender.<sup>85</sup> Often, apps access more data than they need to function—for example, an app promoting artist Jay-Z’s 2013 album required consumers to agree to share precise GPS location and provide access to email and social media accounts before consumers could listen to the music.<sup>86</sup> Apps may also have access to personal information of individuals who have never even used the software. For example, Facebook not only provides third-party applications with personal information about a user, including political affiliation, relationship information, contacts, photos, identity, and location, but that of their Facebook “friends” too.<sup>87</sup>

### **ACLU Facebook app shows consumers how much personal information Facebook apps get—**

It was not until the ACLU of Northern California released an app about Facebook apps that many users realized just how much of their personal information was falling into the “app gap” and ending up in the hands of third party developers.<sup>88</sup> When Facebook released its platform for app developers in 2007, it also provided them default access to a wide range of personal information not only about the individual who ran the app but about their Facebook “friends” too.<sup>89</sup> This information could include political affiliation, relationship information, contacts, photos, identity, and location.<sup>90</sup> The ACLU’s app brought much-needed attention to the issue and Facebook was forced to take some preliminary steps to improve app privacy by directing apps to ask for user permission, though still not that of friends, before accessing user data.<sup>91</sup>

Recent investigations have also found that many mobile apps are sharing personal information with third parties.<sup>93</sup> By surveying 101 popular apps, researchers found that more than half were sharing personal information with other companies without consumers’ knowledge or consent.<sup>94</sup> The apps collected and sent information such as political affiliation, relationship information, contacts, photos, real name, and location to ad networks.<sup>95</sup> For example, popular “free” apps such as Pandora radio<sup>96</sup> and MyFitnessPal collect and transmit age, gender, location, and phone IDs to advertising companies, analytics services, and other third parties that track users.<sup>97</sup> This practice is widespread: in 2012, a risk assessment company discovered that more than half of the top “free” iOS (Apple) and Android apps share information with third-party ad networks or data analytics companies.<sup>98</sup> Other companies embed tracking software into apps, allowing for the creation of detailed profiles such as “wealthy bookworms who own small businesses or new mothers who travel for business and like to garden.”<sup>99</sup> With 19 percent of smartphone owners using apps for health purposes as of 2012,<sup>100</sup> and 29 percent using smartphone for mobile banking purposes,<sup>101</sup> there is a risk that the information collected and shared will be very sensitive in nature.

**"Your personal privacy should not be the cost of using mobile apps, but all too often it is."<sup>92</sup>**

**—California Attorney General Kamala D. Harris**

Apps are also collecting and sharing children’s information. A 2012 Federal Trade Commission study of 500 apps aimed at children discovered that 59 percent transmitted location information, mobile device ID, or phone numbers to a third party.<sup>102</sup> Many of these services and applications share personal information with advertisers and other third parties.<sup>103</sup> In 2012, the FTC fined mobile online journal app Path for collecting the birthdays and phone numbers from children without parental consent.<sup>104</sup>

# PART II: Is Shine the Light Giving Consumers Transparency?

Data brokers, online advertisers, and third-party applications all collect and share information in ways California legislators could not have envisioned in 2003 when they passed Shine the Light. With the passage of time, initial optimism over Shine the Light's potential has faded. Today, multiple studies reveal that customers are unable to use the law to learn how their personal information has been collected and shared.

Early research showed great promise for Shine the Light. A 2004 survey of 32 for-profit companies revealed that the law's passage had already motivated 69 percent of the companies to "tighten information-sharing practices and controls with marketers."<sup>105</sup> Forty-one percent of those same companies said they planned to "seriously consider adopting a 'do not share' policy with third-party marketers." The majority of surveyed companies expressed confidence that they would be able to comply with the law.<sup>106</sup>

But in more recent years, a series of studies of the law by the California Public Interest Research Group (CalPIRG) in 2006, UC-Berkeley researchers in 2007 and 2009, and the ACLU of Northern California in 2012, have each demonstrated the law's failure to achieve its goals. These efforts revealed significant loopholes and limitations in the current law and how they leave consumers in the dark about the way businesses share their information. Shine the Light's shortcomings include everything from the method by which companies tell consumers about their rights, to the process Californians must follow to request transparency, to loopholes in the law that disfavor consumers, to the actual scope of a company's transparency obligation under the law. These weaknesses prevent consumers from obtaining a meaningful picture of how companies collect and share their personal information.

## Shine the Light Requests Are Difficult to File

Customers attempting to use Shine the Light may find it difficult because many companies do not properly notify consumers of their rights or how to send a request under the law. The law directs businesses to tell users about their rights and provide a contact point where Shine the Light requests may be submitted, such as a mailing address.<sup>107</sup> Having companies follow these notice requirements is important because a business is given 150 days, or five months, to respond a request sent to a non-designated address.<sup>108</sup> If a business places its contact information under the heading "Your California Privacy Rights," it need not respond at all to a request sent to a different address.<sup>109</sup> A majority of the 112 companies in the 2009 Berkeley study did not specify any contact information specifically for Shine the Light.<sup>110</sup> Two businesses, K-Mart and the New York Times, actually provided incorrect contact information.<sup>111</sup> In the ACLU-NC's 2012 study, members could not find Facebook's Shine the Light contact information, and the company did not return emails asking for the error to be fixed.<sup>112</sup>

## Responses May Come Late or Never at All, or Have Inadequate Information

Research has also found that even when Californians are able to correctly submit requests, Shine the Light responses may come late, or never at all. In CalPIRG's 2006 study, only 31 of 52 participants sending requests received some sort of response within the required time frame.<sup>113</sup> Twenty participants received no response at all.<sup>114</sup> Businesses ignored 10 of the 86 requests made by UC-Berkeley researchers in 2007, and the response rate was even worse in its 2009 follow-up study, where 55 of the 112 companies failed to "respond in any manner."<sup>115</sup>

Much of the blame lies with the law's convoluted response rules that make it hard for a consumer to learn if the business is failing to properly respond or is not required to respond. A company only has to respond to a Shine the Light request if it has shared personal information with a third party and knows or reasonably should know that the third party used the personal information for direct marketing purposes.<sup>116</sup> Matters are further complicated by additional provisions that also create disparate timing response rules. Generally, a business must respond within 30 days after receiving the request, either by listing what categories of personal information they have shared with what third party businesses for direct marketing purposes, or by providing the consumer with information about how to opt-out of future information sharing.<sup>117</sup> But if a company fails to respond, there is no consequence as long as it sends a response within another 90 days after learning of the error.<sup>118</sup> Further, the company is given 150 days, or five months, to respond a request sent to a non-designated address.<sup>119</sup>

For consumers that actually make it through the law's hurdles and receive a response, many are left to sort through inadequate or confusing information. Some companies, including 22 of the 86 companies that Berkeley researchers contacted in 2007, responded with a copy of their privacy policy rather than the information required by the law.<sup>120</sup> In response to a Shine the Light request made as part of the ACLU-NC's study, Yahoo! wrote, "[P]lease see our Privacy Policy," rather than describing what the policy says—that Yahoo! shares personal information with "trusted partners" for offering products and services to users.<sup>121</sup> And some companies provided inconsistent responses to the same request. Requests sent to Amazon by participants in the ACLU-NC study resulted in varying responses, with one stating that the consumer should contact the legal department, another describing that the information Amazon shares "varies depending on the nature of [a] particular partner's business," and yet another discussing account security.<sup>122</sup> It is not surprising then that half of the people who received a Shine the Light response in CalPIRG's 2006 study said they "were not satisfied" with it.<sup>123</sup>

## Consumers May Only Learn How Their Personal Information Is Shared for "Direct Marketing Purposes"

With Shine the Light, Californians can only learn about how their personal information has been shared for "direct marketing purposes," which is limited to the direct sale or leasing of goods or services through postal mail, telephone, or email.<sup>124</sup> Many business practices in the modern digital age, including targeted advertising and purchases of consumer information by data brokers, fly under the radar. In UC-Berkeley's 2009 study, 39 of the 59 responders responded with no information beyond an assertion that personal information was not shared for direct marketing purposes.<sup>125</sup> Seven of

the nine companies reached by the ACLU-NC's 2012 study also failed to provide any information about how they share personal information with third parties for reasons other than direct marketing purposes.<sup>126</sup> However, six of these companies actually do share information with third-party advertisers or allow third parties to install cookies on users' computers, according to each company's privacy policies.<sup>127</sup> In fact, three of these companies—Verizon, Yahoo!, and Apple—may also share customer information with other third parties such as affiliates and “trusted partners.”<sup>128</sup>

## Businesses Get an Easy Out if They Provide an “Opt-Out”

The law also allows a business to avoid responding to a request with information about sharing practices as long as it gives the consumer the option to opt out of future sharing.<sup>129</sup> If a business provides this opt-out option, the consumer is not entitled to learn what personal information the company has already shared. Twenty-two of the 86 companies responded to UC-Berkeley's 2007 survey with the opt-out option and a copy of their privacy policy, which outlines only general practices.<sup>130</sup> Five companies in the 2009 Berkeley survey provided the opt-out option even though four sold consumer data online.<sup>131</sup> When the ACLU-NC's study participants sent requests in 2012, LinkedIn asserted that even if it did share information for direct marketing purposes, it would not need to disclose those practices because it provides an opt-out.<sup>132</sup> This opt-out feature of the law gives businesses an easy out—a business that provides the option can end up sharing consumer information without transparency, and then point to an opt-out option if they receive a request for information.<sup>133</sup>

## Shine the Light Does Not Provide Transparency for the Sharing of Many Types of Personal Information

Consumers cannot use Shine the Light to learn how a business shares many sensitive types of personal information. The law's definition of personal information is a limited list and lacks many types of information, including location information and sexual orientation.<sup>134</sup> With 92 percent of Californians carrying cell phones, all of which produce location information about where Californians live, work, and travel, not knowing if this sensitive information is being shared with third parties can lead to dangerous outcomes.<sup>135</sup> Several women and children have been hurt or killed when cell providers or applications collected and then shared location data with abusers, and more than 25,000 adults in the U.S. are already victims of GPS stalking annually.<sup>136</sup> Large numbers of Californians are also increasingly turning to the Internet and mobile devices to access information about personal issues, from sexuality to health.<sup>137</sup> The law's outdated definition of personal information makes it possible for online services to collect and disclose sexual orientation, for apps to disclose location, and for medical devices to collect sensitive health information, all without having to reveal it to a Californian who uses Shine the Light to try to learn how their personal information is shared.

**Online dating sites share sensitive about their users.** It was revealed in 2012 that the online dating site OK Cupid collects and shares sexual orientation information with two companies and drug-use statistics with six.<sup>138</sup> A researcher also determined that the site—which utilizes advertising as part of its business model—shares personal information including age, drug use, drinking frequency, ethnicity, gender, income, relationship status, and religion with some of its marketing partners.<sup>139</sup>

## Consumers Cannot Learn about Sharing with Separately-Branded Affiliates or Business Partners

Shine the Light requires businesses to reveal information sharing with “third parties.” But the definition of a “third party” in the current law is quite narrow and does not cover many businesses that do not share a brand name or common branding such that an affiliate relationship would be clear to a customer.<sup>140</sup> This narrow definition allows many companies to share personal information with business affiliates, sister companies, and even “trusted partners” that many consumers would assume are third parties, without having to reveal this information to California consumers.<sup>141</sup> For example, Berkeley’s 2009 study found that the craft store Michaels used the term “affiliates” to refer to “apparent third parties.”<sup>142</sup> A response by Verizon as part of the ACLU-NC study stated that the phone company does not share personal information “with third parties outside the Verizon family of companies,” yet its privacy policy reveals that this includes all Verizon telephony corporations and Redbox Instant, a video streaming service Californians may not know is associated with or exchanges information with the phone company.<sup>143</sup>

## Companies that Do Not Have an “Established Business Relationship” with Consumers Are Not Subject to Shine the Light

Under Shine the Light, only customers that can demonstrate an “established business relationship” with a business, perhaps through buying or selling something through the business, may learn how their personal information is shared.<sup>144</sup> This “established business relationship” requirement limits consumers’ ability to use the law because modern digital businesses often do not give rise to circumstances that establish a traditional “business relationship.”

For example, many actors in the targeted advertising ecosystem may lack an “established business relationship” with consumers. Actors that collect and share the personal information of consumers by tracking online activities or selling advertisements may fall outside the law’s scope entirely.<sup>145</sup> In the same way, third parties that use trackers to follow consumers across various sites or to serve individually tailored ads may not have an “established business relationship,” nor may data brokers that buy information from third parties—both online and off—and can compile profiles of consumers without any contact with the individual.<sup>146</sup>

Companies use the business relationship requirement to avoid providing information to California consumers. Four of the nine businesses that did not respond with information in UC-Berkeley’s 2007 study claimed no such business relationship existed or that “that the requestor was under an affirmative duty to prove that one existed.”<sup>147</sup> In Berkeley’s 2009 study, Continental Airlines, Pizza Hut, and Hyatt requested evidence of an “established business relationship” before they would respond.<sup>148</sup> In all, nine companies in the 2009 study either disputed whether an “established business relationship” existed or provided incomplete responses.<sup>149</sup>

# PART III: Consumer Transparency Measures Enjoy State, National, and International Support

Now is a very good time to evaluate the Shine the Light law and the ways it can be improved because state, federal and international policymakers, and increasingly businesses, are recognizing the importance of providing consumers with transparency into corporate information practices.

## California Support for Transparency

Efforts to improve transparency about the collection and sharing of personal information by businesses are picking up steam at the state level. The Select Committee on Privacy for the California Assembly convened an informational hearing on digital privacy in the spring of 2013 that included discussion about the lack of consumer information regarding information collection, use, and disclosure.<sup>151</sup> California lawmakers also introduced several important online privacy and transparency bills in 2013.<sup>152</sup>

**“Protecting the privacy of online consumers is a serious law enforcement matter.”<sup>150</sup>**

**—California Attorney General  
Kamala D. Harris**

California Attorney General Kamala Harris has actively enforced current California transparency laws, brokered agreements to increase transparency, and provided guidance for companies to increase access and transparency. In 2012, her office announced the enforcement of the California Online Privacy Protection Act<sup>153</sup> against smartphone apps, thus requiring app developers to conspicuously post a privacy policy complying with the law.<sup>154</sup> The Attorney General also negotiated an agreement with major platforms that host mobile applications to make privacy policies available prior to download. The agreement promises to “provide more transparency and [to] give mobile users more informed control over who accesses their personal information and how it is used.”<sup>155</sup> In 2013, the Attorney General’s office also released “Privacy on the Go – Recommendations for the Mobile Ecosystem,”<sup>156</sup> a guide that called on the mobile business community to provide greater transparency and data access rights to consumers.<sup>157</sup>

## National Support for Transparency

There has been a significant push for greater transparency at the federal level as well by lawmakers, regulators, and the executive branch. In particular, the Federal Trade Commission (FTC) has been active in promoting transparency. In 2012, it released best-practice guidelines that encouraged corporations to give consumers greater control over the collection and use of their personal data through simplified choices and increased transparency, and suggested providing consumers with access to their data in a manner proportionate to the sensitivity and nature of its use.<sup>158</sup> In June of 2013, FTC Commissioner Julie Brill called for a comprehensive initiative called “Reclaim Your Name,” that would allow consumers access to their information held by data brokers, as well as a means to opt out of any uses of the data for marketing purposes and to correct errors before they are relied upon by others.<sup>159</sup> The agency has also called on Congress to pass a law giving consumers access to the information data brokers hold<sup>160</sup> and has issued reports critiquing companies that collect and share children’s information from mobile devices without proper transparency and consent.<sup>161</sup> Edith Ramirez, Chairwoman of the FTC, calls transparency the “key to accountability, the key to responsible

data collection and use, and the key to building consumer trust,” and supports measures that “enable consumers to know what information is being collected and with whom that information is being shared.”<sup>162</sup>

Federal policymakers and regulators also recognize the dangers posed by the opaque collection and sharing of consumer information, including by data brokers.<sup>164</sup> In July 2012, eight U.S. members of Congress sent letters to top data brokers demanding to know how they gathered and shared information.<sup>165</sup>

According to a joint statement by the eight lawmakers, the data brokers’ responses left many questions “unanswered” and only gave “a glimpse of the practices of an industry that has operated in the shadows for years.”<sup>166</sup> The Senate Commerce Committee, led by Senator John D. Rockefeller IV, opened its own investigation into data broker practices in October 2012 and expanded the inquiry in September 2013 by calling on 12 popular websites to reveal whether they share information with data brokers.<sup>167</sup> Individual members of Congress have also pursued efforts to bring increased transparency to other aspects of data sharing. For example, Sen. Ed Markey (D-MA) has called on mobile phone carriers to disclose detailed information about the records and data that they share with law enforcement agencies.<sup>168</sup>

**“[I]t is difficult today for consumers to assess whether a company’s privacy practices warrant their trust.”<sup>163</sup>**

**—The White House’s Consumer Data Privacy Framework**

The Obama Administration has also recommended additional transparency measures. In February 2012, The White House released a Data Privacy Framework that included a Consumer Privacy Bill of Rights setting forth a “blueprint for privacy.”<sup>169</sup> The document specifically calls on advocates, industry players, and lawmakers to enact enforceable codes of conduct and laws that provide consumers with meaningful transparency, individual control, and a right to access.<sup>170</sup> It recommends that companies, including data brokers, clearly and honestly describe in their privacy statements how they collect, use, and share consumer data, and that they provide consumers with the means to view and correct their data.

## International Support for Transparency

The United States has lagged behind both Canada and Europe for decades in providing transparency and access rights to consumer data. Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) recognizes individual privacy interests and sets forth principles that govern how companies collect, obtain consent for collection, and retain personal information, including an individual right of access to relevant personal information.<sup>172</sup> In 2013, Canada’s Privacy Commissioner called for an update to PIPEDA that would provide for further transparency.<sup>173</sup> As the Privacy Commissioner noted, the goals of this update effort are both to protect privacy and support innovation, because “getting privacy right can be a competitive advantage—it can help encourage trust.”<sup>174</sup>

**“Data protection in Europe is a fundamental right ... Strong rules allow trust and, in the Internet world, without trust you cannot go ahead.”<sup>171</sup>**

**—EU Vice President & Commissioner Viviane Reding**

Europeans currently have even greater transparency and access rights. Since 1995, the European Data Protection Directive<sup>175</sup> has provided European residents the right to access data held and shared by companies and third parties.<sup>176</sup> The scope of the access right has been interpreted broadly—for example, IP addresses are considered to be personal data in certain circumstances.<sup>177</sup> The Directive also provides residents the right to object to a company’s use of personal data, including for marketing purposes.<sup>178</sup> In 2012, the European Commission announced proposed reforms that would

expand and strengthen the Directive, including easier-to-understand responses to access requests, data portability, and the provision of notice to consumers about data retention periods.<sup>179</sup>

American businesses operating in Europe must already provide the transparency required by these laws. Some large American companies such as Facebook and Google maintain automated portals to help provide certain, limited information to consumers. For example, a Facebook user can request an archive of their account and receive an email from Facebook with a link to a file containing private Wall posts, chat histories, IP addresses used to access the service, photos, profile information, and even facial recognition data.<sup>180</sup> Google's similar service—Takeout—gives users a way to instantly download their Drive cloud storage, contacts, blog entries, and Google Voice metadata.<sup>181</sup>

Though studies of the European right of access also show some needed areas of improvement, individuals are able to use the current laws to obtain far greater access than Californians using the Shine the Light law. In 2006, a Finnish researcher utilized the free right of data access in his country to make 41 company requests.<sup>182</sup> He received 29 responses, the vast majority arrived in a timely manner, and contained statements of the entities' data practices as well as screen-shots, faxes, email printouts, and signed letters related to his personal data.<sup>183</sup> Another Europe-wide study of the right of access noted that while companies claimed that it would be difficult to comply with information requests by consumers, those concerns were generally not borne out in practice.<sup>184</sup>

In recent years, Europeans have been able to effectively use their access rights to get a glimpse into the vast amounts of personal information that both social networking and mobile companies are collecting and retaining. The transparency enabled by the European system can bring real change, from the Austrian student who shocked the Facebook community after using his access right to reveal Facebook's massive dossier on him, to the German politician who used the right to highlight to the public the vast amount of location data that mobile companies collect every day.<sup>185</sup>

**EU Right of Access reveals Facebook collected 1,200 pages of data on student.** Max Schrems, an Austrian law student, used his EU right of access to learn that Facebook had collected 1,200 pages of data about him in just three years. His dossier included all his friend-ing and un-friending, all the events he had been invited to and his responses, all of his past messages and chats (even those he had "deleted"), and email addresses he had never even provided to the company. Following these revelations, Irish authorities conducted a privacy audit of Facebook and the company was pressured to make privacy changes, including a privacy tutorial for all new users that educates individuals on data privacy issues like default settings and data access.<sup>186</sup>

**German politician finds cell phone company had tracked him every seven seconds.** Malte Spitz, a German Green Party politician, was able to use the EU right of access to learn just how much location data his cell phone company, Deutsche Telekom, collected about him. Spitz forced his cell company to reveal that it had over 35,000 data points about him, plotting his location every seven seconds, over a six-month period. When Spitz released the records publicly, it not only caused public embarrassment for the company, but the German Constitutional Court declared it illegal for the records to be retained for such a long period. Deutsche Telekom "immediately ceased" storing any location data related to customers' phones.<sup>187</sup>

## Corporate Support for Transparency

Businesses are also increasingly talking about the importance of consumer transparency and access rights and some are starting to take action to back up those statements.<sup>188</sup> Facebook, Google,<sup>189</sup> and Twitter<sup>190</sup> allow users to download copies of their own data. In May 2013, LinkedIn announced it would provide its users with a “Privacy Portal”—a single place where users would be able to access all their data on the service.<sup>191</sup> In September 2013, data broker Acxiom rolled out an online portal that gives consumers a limited glimpse of the information the company knows about them.<sup>192</sup> Amazon, Google, and Yahoo! also provide some transparency about personalized advertisements, enabling consumers to learn the interest groups that they have been classified under by the company, change advertising preferences, or opt out of the companies’ targeted advertising altogether.<sup>193</sup> Facebook’s CEO Mark Zuckerberg has stated he is “committed to making Facebook the leader in transparency and control around privacy.”<sup>194</sup> At Microsoft, General Counsel Brad Smith has noted “we cannot have privacy if there is no transparency.”<sup>195</sup> In July 2013, Forrester Research predicted that privacy would be the next “green movement,” with companies competing for business with policies that respect consumer data.

**Privacy will be the next  
“green movement” with  
companies competing for  
business with policies that  
respect consumer data.**

**—Forrester Research**

There is also a new movement by large technology companies to provide transparency about government demands for information. In 2009, Google became the first major company to issue a transparency report, publicly reporting every six months on the number of demands it receives from U.S. law enforcement for user data, the number of accounts affected, and how often Google disclosed the information to government officials.<sup>196</sup> Twitter and Dropbox followed suit with their own transparency reports in 2012 and Microsoft did the same in early 2013.<sup>197</sup> In June 2013, following the revelations by whistleblower Edward Snowden about widespread NSA spying,<sup>198</sup> Yahoo!, Facebook, and Apple issued their first transparency reports.<sup>199</sup> Facebook and Yahoo! followed up in August 2013 with global transparency reports.<sup>200</sup>

Policymakers are increasingly supporting efforts to improve transparency and some high-profile companies are also beginning to provide some transparency to consumers. But transparency practices must still expand dramatically in both scope and reach for consumers to be properly informed about how companies collect and share their information.

# PART IV: A Common-Sense Update for Shine the Light

Rapidly changing technology, research on Shine the Light, and the interest of both policymakers and businesses in transparency show that even though Shine the Light was groundbreaking when enacted in 2003, the time has come to update California law to provide consumers with meaningful transparency in the modern digital world.

Based on Shine the Light's limitations and the changed nature of information practices in the modern digital world, we have developed several principles for updating California privacy law to provided needed transparency for consumers. This framework would modernize, strengthen, and streamline California transparency law so it can work effectively and efficiently for both consumers and companies. Whether Californians search online, shop at retail, or use a mobile app, they should be able to learn if their personal information related to health, finances, location, and more, is being collected and shared with other companies, including targeted advertisers, data brokers, and third-party applications. A modern transparency law that follows these principles will enable Californians to learn the "who what, where, and when of how a business handles personal information" and place them in a position to take more privacy-protective steps.

## Give Consumers the Right to Learn What Personal Information Companies Collect and Disclose about Them



**Require a company to respond at least once per year to a customer's request for an accounting of the personal information held about them by the company.**

Access rights are endorsed by the FTC, the White House's Consumer Privacy Bill of Rights, and the California Attorney General.<sup>201</sup> Some American companies with EU customers must already provide access to all collected personal information and right now, some companies already have automated portals that allow Americans to access this information too.<sup>202</sup>



**Require companies to provide a substantive response to requests for information even if the company also allows consumers to opt out of data collection or sharing.**

The current Shine the Light law allows companies to choose between being transparent about their data disclosure practices and providing consumers with some sort of mechanism to opt out of future disclosures. This creates a loophole allowing companies to avoid revealing certain practices to consumers by providing an opt-out mechanism, even if consumers are not previously aware of this option. A modern transparency law should ensure that companies reveal data collection and disclosure practices.

## Provide Transparency for All Modern Information Collection and Disclosure



**Modernize the scope beyond "direct marketing purposes" to cover modern business practices.**

In the modern digital world, all collection and sharing should be covered by the transparency law since a wide variety of companies are in a position to collect, obtain, and disclose personal information to many different types of entities.



**Modernize the definition of “personal information” to make it consistent with modern technology and business practices.**

Modern technology allows companies to collect and disclose a wide variety of sensitive personal information. Instead of a narrow and under-inclusive list of categories, the definition should cover all types of personal information (including location information, buying habits, and sexual orientation), and be consistent with current California law<sup>203</sup> and the FTC’s 2012 privacy guidelines, which cover all information “reasonably linked” to a consumer.<sup>204</sup>



**Modernize the definition of customer by eliminating the “established business relationship” so consumers can learn about information collected or shared by modern online businesses.**

Many online businesses, including data brokers, third-party apps and online advertisers, collect and disclose information about individuals with whom they have little to no direct contact and potentially no established business relationship. The law should be updated to ensure that transparency requirements are not based on whether there is an “established business relationship,” but are triggered by the fact that a company retains or shares a consumer’s personal information.



**Update the definition of “third party” to match consumer expectations and simplify compliance.**

The definition of third party should mirror the FTC’s suggested definition, allowing consumers to learn how their personal information is disclosed to any entity that does not share common branding or have a relationship that would be otherwise clear to a customer.<sup>205</sup> At the same time, an update should clarify the law and make compliance easier for companies by removing an additional transparency requirement triggered when companies share certain personal information with affiliate third parties.<sup>206</sup>

## Have Simple and Efficient Request and Response Requirements



**Make it easy for customers to learn about their rights and properly send requests.**

Shine the Light would be a more effective tool if it were simpler for consumers and companies to understand and use. An update should have streamlined technical notice requirements, require a notice of rights under the law in existing privacy policies, and ensure that employees responding to inquiries are informed about how the process works.



**Require companies to respond to a request within 30 days.**

Current law provides for various deadlines for response depending on the address to which a request is sent; moreover, it allows companies to send no response at all if they believe they are not covered under the law. An updated transparency law should require all companies that collect or disclose personal information to respond to a request within 30 days.



### **Enable flexible means for companies to respond to requests.**

Current law requires companies to respond to a request “in writing or by electronic mail,” excluding the possibility of more responsive and efficient mechanisms for responding to requests. A modern transparency law should give companies the flexibility to select the most efficient and effective way to provide required information, whether by email, via an automated web portal similar to those already in use by companies for existing EU transparency requirements, or another means.



### **Require that a company provide a response describing its retention and disclosure of the requesting consumer’s specific personal information when this information is reasonably available.**

A transparency law should augment the general descriptions of a company’s data retention and disclosure practices that are included in privacy policies by providing transparency of personal relevance to an individual that behavioral research suggests is more effective.<sup>207</sup> As such, an update should require personalized responses whenever that information is reasonably available.

## **Make Sure Transparency Law Is Consistent with Legitimate Business Practices and Can Be Fairly Enforced**



**Ensure that the law does not apply to data collection and sharing exclusively for purposes such as online security and threat detection.**



**Improve company compliance and enforcement mechanisms by making it clear that violations of the law constitute an injury and companies will be liable for penalties.**



**Maintain reasonable penalty provisions as well as a cure period for companies to address problems prior to being liable for penalties.**



**Recognize the need to balance transparency interests with privacy and security by allowing companies to refuse to provide information to customers whose identity cannot be reasonably verified.**

## **CONCLUSION**

California’s landmark Shine the Light law is showing its age after a decade of exponential technological innovation and changed business practices. Today, the law’s structural deficiencies and outdated scope fail to provide Californians with needed transparency about who has and who shares their personal information. With Californians deeply concerned about the privacy of their personal information and broad support of policymakers for increased transparency and access rights, now is the time to update transparency law for the modern digital era.

# ENDNOTES

- <sup>1</sup> Senate Judiciary Committee Analysis of SB 27, May 7, 2003, available at [http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb\\_0001-0050/sb\\_27\\_cfa\\_20030507\\_132723\\_sen\\_comm.html](http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_0001-0050/sb_27_cfa_20030507_132723_sen_comm.html); see Senate Bill 27, available at [http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb\\_0001-0050/sb\\_27\\_bill\\_20030925\\_chaptered.pdf](http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_0001-0050/sb_27_bill_20030925_chaptered.pdf).
- <sup>2</sup> CAL. CIV. CODE § 1798.83, available at <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84>.
- <sup>3</sup> Press Release, USC Dornsife/Los Angeles Times, Voters Across the Political Spectrum Concerned About Tech Companies Invading Their Privacy (Mar. 31, 2012) available at <http://dornsife.usc.edu/usc-lat-poll-privacy-march-2012/>.
- <sup>4</sup> 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](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214).
- <sup>5</sup> CAL. CONST. art. 1, § 1.
- <sup>6</sup> Press Release, USC Dornsife/Los Angeles Times, Voters Across the Political Spectrum Concerned About Tech Companies Invading Their Privacy (Mar. 31, 2012) available at <http://dornsife.usc.edu/usc-lat-poll-privacy-march-2012/> [hereinafter USC Dornsife/Los Angeles Times]; Joel Kelsey & Michael McCauley, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, CONSUMER'S UNION (Sept. 25, 2008), [http://www.consumersunion.org/pub/core\\_telecom\\_and\\_utilities006189.html](http://www.consumersunion.org/pub/core_telecom_and_utilities006189.html) (57 percent of consumers in a 2008 Consumer Union study incorrectly believed that companies must identify themselves and indicate why they are collecting data and whether they intend to share it with other organizations); OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE (Annenberg Public Policy Center of the University of Pennsylvania, Jun. 1, 2005), available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31> (59 percent of participants in a 2005 study believed, falsely, that websites with a privacy policy cannot sell personal information without consent, according to research by Professor Joseph Turow).
- <sup>7</sup> USC Dornsife/Los Angeles Times, *supra* note 6.
- <sup>8</sup> *Id.*
- <sup>9</sup> Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. OF L. & SOC. CHANGE 215, 266, 270 (2012) available at <http://ssrn.com/abstract=2083733> [hereinafter Ozer] citing KPMG CONSUMERS AND CONVERGENCE IV, CONVERGENCE GOES MAINSTREAM: CONVENIENCE EDGES OUT CONSUMER CONCERNS OVER PRIVACY AND SECURITY 6 (2010), available at <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/consumers-andconvergence/Documents/Consumers-Convergence-IV-july-2010.pdf>.
- <sup>10</sup> 38% list privacy as the most significant concern about their device. Kristina Knight, *Mobile Consumers Most Concerned About Privacy*, BIZREPORT (Apr. 27, 2011), <http://www.bizreport.com/2011/04/survey-mobile-consumers-most-concerned-about-privacy.html>.
- <sup>11</sup> See Kenneth Rapoza, *Socially Networked: 52% of Americans on Facebook, Similar Sites*, FORBES (June 1, 2011, 10:52 PM), <http://blogs.forbes.com/kenrapoza/2011/06/01/socially-networked-52-of-americans-on-facebook-similar-sites/>.
- <sup>12</sup> ANONYMITY, PRIVACY, AND SECURITY ONLINE, (Pew Internet & American Life Project, Sept. 5, 2013), available at [www.pewinternet.org/Reports/2013/Anonymity-online.aspx](http://www.pewinternet.org/Reports/2013/Anonymity-online.aspx).
- <sup>13</sup> See TUROW ET AL., *supra* note 4.
- <sup>14</sup> Chris Jay Hoofnagle, Jennifer King, Su Li & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* 17-19 (Working Paper, Apr. 2010), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1589864](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864). Young adults fared even worse in the survey, with 88 percent of respondents aged 18 to 24 answering two or fewer questions correctly.
- <sup>15</sup> Joel Kelsey & Michael McCauley, *Consumer Reports Poll: Americans Extremely Concerned About Internet Privacy*, CONSUMER'S UNION (Sept. 25, 2008), [http://www.consumersunion.org/pub/core\\_telecom\\_and\\_utilities006189.html](http://www.consumersunion.org/pub/core_telecom_and_utilities006189.html).
- <sup>16</sup> The 2007 Golden Bear Omnibus Survey was a random-digit telephonic survey of 1,186 English and Spanish speaking adults in California. It was conducted by the University of California's Survey Research Center using Computer-Assisted Telephone Interviewing (CATI) to landline and wireless phones from Apr. 30, 2007-Sept. 2, 2007. It was funded by the Survey Research Center, and the Samuelson Clinic funded these questions focusing on privacy. See JOSEPH TUROW, DEIRDRE K. MULLIGAN & CHRIS JAY HOOFNAGLE, RESEARCH REPORT: CONSUMERS FUNDAMENTALLY MISUNDERSTAND THE ONLINE ADVERTISING MARKETPLACE (Oct. 2007), available at [http://www.law.berkeley.edu/clinics/samuels/annenberg\\_samuels\\_advertising-11.pdf](http://www.law.berkeley.edu/clinics/samuels/annenberg_samuels_advertising-11.pdf); Chris Jay Hoofnagle & Jennifer King, *What Californians Understand about Privacy Online* 12 (Sept. 3, 2008), available at <http://ssrn.com/abstract=1262130>; JOSEPH TUROW, LAUREN FELDMAN, & KIMBERLY MELTZER, OPEN TO EXPLOITATION: AMERICAN SHOPPERS ONLINE AND OFFLINE (Annenberg Public Policy Center of the University of Pennsylvania, Jun. 1, 2005), available at <http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31>.
- <sup>17</sup> KRISTEN PURCELL, JOANNA BRENNER, & LEE RAINIE, SEARCH ENGINE USE 2012: SUMMARY OF FINDINGS (Pew Internet & American Life Project, Mar. 9, 2012), available at <http://pewinternet.org/Reports/2012/Search-Engine-Use-2012/Summary-of-findings.aspx>.
- <sup>18</sup> Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 1, 17 (2008), quoted in Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 297 (2011).
- <sup>19</sup> FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 2 (2012), available at <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> [hereinafter FTC PRIVACY RECOMMENDATIONS].
- <sup>20</sup> *Id.* at 61.
- <sup>21</sup> Ina Fried, *Interview: Apple CEO Steve Jobs on How the iPhone Does and Doesn't Use Location Information*, ALL THINGS DIGITAL (Apr. 27, 2011, 9:55 AM), <http://allthingsd.com/20110427/exclusive-apple-ceo-steve-jobs-on-how-the-iphone-does-and-doesnt-use-location-information/>.
- <sup>22</sup> Jeff John Roberts, *Privacy as the next green movement? Study says companies will compete on data practices*, GIGAOM, July 29, 2013, <http://gigaom.com/2013/07/29/privacy-as-the-next-green-movement-study-says-companies-will-compete-on-data-practices/>.
- <sup>23</sup> See TUROW ET AL., *supra* note 4, at 3.
- <sup>24</sup> SASHA ROMANOSKY, RICHARD SHARP, ALESSANDRO ACQUISTI, DATA BREACHES AND IDENTITY THEFT: WHEN IS MANDATORY DISCLOSURE OPTIMAL? (Carnegie Mellon University - Heinz College of Information Systems and Public Policy, 2012), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1989594](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989594).
- <sup>25</sup> JAN LAUREN BOYLES, AARON SMITH, MARY MADDEN, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (Pew Internet & American Life Project, Sept. 5, 2012), available at [http://pewinternet.org/~media/Files/Reports/2012/PIP\\_MobilePrivacyManagement.pdf](http://pewinternet.org/~media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf).
- <sup>26</sup> *Id.*
- <sup>27</sup> JANICE TSAI, SERGE EGELMAN, LORRIE CRANOR & ALESSANDRO ACQUISTI, THE EFFECT OF ONLINE PRIVACY INFORMATION ON PURCHASING BEHAVIOR: AN EXPERIMENTAL STUDY 7, (ICIS 2007 Proc. 2007), available at <http://www.heinz.cmu.edu/~acquisti/papers/acquisti-onlinepurchasing-privacy.pdf> (pre-publication version).
- <sup>28</sup> *Id.* at 7.
- <sup>29</sup> *Id.* at 25.
- <sup>30</sup> *Id.* at 35.
- <sup>31</sup> CHRIS HOOFNAGLE, BEYOND GOOGLE AND EVIL: HOW POLICY MAKERS, JOURNALISTS AND CONSUMERS SHOULD TALK DIFFERENTLY ABOUT GOOGLE AND PRIVACY, FIRST MONDAY Vol. 14, No. 4-6, April 6, 2009, available at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1380702](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1380702).
- <sup>32</sup> WILLIAM K. DARLEY & JEEN-SU LIM, PERSONAL RELEVANCE AS MODERATOR OF THE EFFECT OF PUBLIC SERVICE ADVERTISING ON BEHAVIOR, ADVANCES IN CONSUMER RESEARCH Volume 18, 1991, available at <http://www.acrwebsite.org/search/view-conference-proceedings.aspx?Id=7177>
- <sup>33</sup> Larry Ponemon, *Shining the Light on Our Personal Information*, DARWIN MAGAZINE, Sept. 1, 2004, (this publication can be obtained from the Internet Archive's Way Back Machine at <http://web.archive.org/web/20041118164240/http://www.darwinmag.com/read/feature/column.html?ArticleID=1158>).
- <sup>34</sup> NATIONAL CONFERENCE OF STATE LEGISLATORS, STATE SECURITY BREACH NOTIFICATION LAWS (Aug. 20, 2012) available at <http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx>.
- <sup>35</sup> PAUL M. SCHWARTZ & EDWARD J. JANGER, NOTIFICATION OF DATA SECURITY BREACHES 956-58, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=908709](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=908709); PROFESSOR DEIRDRE K. MULLIGAN & KENNETH A. BAMBERGER, SECURITY BREACH NOTIFICATION LAWS: VIEWS FROM CHIEF SECURITY OFFICERS 18 (Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law Dec. 2007), available at [http://www.law.berkeley.edu/files/cso\\_study.pdf](http://www.law.berkeley.edu/files/cso_study.pdf). A survey of security professionals released in 2005 showed that security breach notification laws were the most influential regulation in the decision to use encryption.
- <sup>36</sup> CALIFORNIA ATTORNEY GENERAL KAMALA D. HARRIS, DATA BREACH REPORT 2012 (California Department of Justice 2013), available at [http://www.privacyandsecuritymatters.com/files/2013/07/BREACH\\_REPORT\\_2012.pdf](http://www.privacyandsecuritymatters.com/files/2013/07/BREACH_REPORT_2012.pdf).
- <sup>37</sup> SASHA ROMANOSKY, RAHUL TELANG, ALESSANDRO ACQUISTI, DO DATA BREACH LAWS REDUCE IDENTITY THEFT? (Carnegie Mellon University 2008), available at [http://www.heinz.cmu.edu/~rtelang/JPAM\\_MS.pdf](http://www.heinz.cmu.edu/~rtelang/JPAM_MS.pdf) (studying data breaches from 2002-2009); PONEMON INSTITUTE, 2013 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS, available at [https://www4.symantec.com/mktginfo/whitepaper/053013\\_GL\\_NA\\_WP\\_Ponemon-2013-Cost-of-a-Data-Breach-Report\\_daiNA\\_cta72382.pdf](https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf).
- <sup>38</sup> FEDERAL TRADE COMMISSION, BUREAU OF CONSUMER PROTECTION, DIVISION OF FINANCIAL PRACTICES, THE GRAMM-LEACH-BLILEY ACT: PRIVACY OF CONSUMER FINANCIAL INFORMATION, <http://www.ftc.gov/privacy/glbact/glboutline.htm>.
- <sup>39</sup> M. Ryan Calo, *Against Notice Skepticism in Privacy (And Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1060 (2012) quoting Peter Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1313-14, 1316-17 (2002).
- <sup>40</sup> Louis D. Brandeis, *Other People's Money, Chapter V: What Publicity Can Do*, HARPER'S WEEKLY, Nov. 29, 1913, available at <http://www.law.louisville.edu/library/collections/brandeis/node/191>.
- <sup>41</sup> Edith Ramirez, Chairwoman, Federal Trade Commission, Keynote Address (As Prepared for Delivery) at the Technology Policy Institute Aspen Forum (Aug. 19, 2013), available at <http://ftc.gov/speeches/ramirez/130819bigdataaspen.pdf>.
- <sup>42</sup> *Id.* at 10.
- <sup>43</sup> Rainey Reitman, *A Deep Dive into Facebook and Datalogix: What's Actually Getting Shared and How to Opt-Out*, ELECTRONIC FRONTIER FOUNDATION, Sept. 25, 2012, <https://www.eff.org/deeplinks/2012/09/deep-dive-facebook-and-datalogix-whats-actually-getting-shared-and-how-you-can-opt>.
- <sup>44</sup> Cameron Scott, *Facebook to Allow Advertisers to Use Data Broker Data for Ad Targeting*, SOCIAL TIMES, Feb. 22, 2013, available at [http://socialtimes.com/facebook-to-allow-advertisers-to-use-data-broker-data-for-ad-targeting-report\\_b119716](http://socialtimes.com/facebook-to-allow-advertisers-to-use-data-broker-data-for-ad-targeting-report_b119716).
- <sup>45</sup> See Reitman, *supra* note 43.

- <sup>46</sup> Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, June 16, 2012, at BU1, available at <http://www.nytimes.com/2012/06/17/technology/axiom-the-quiet-giant-of-consumer-database-marketing.html>; PRIVACY RIGHTS CLEARINGHOUSE, FACT SHEET 15: WHAT PERSONAL INFORMATION SHOULD YOU GIVE TO MERCHANTS? (Privacy Rights Clearinghouse, rev. Jan. 2013), available at <https://www.privacyrights.org/fs/fs15-mt.htm#4>; Adam Tanner, *Finally You'll Get to See the Secret Consumer Dossier They Have On You*, FORBES ONLINE, June 25, 2013, available at <http://www.forbes.com/sites/adamtanner/2013/06/25/finally-youll-get-to-see-the-secret-consumer-dossier-they-have-on-you/>.
- <sup>47</sup> Rappleaf.com (last visited Oct. 11, 2013).
- <sup>48</sup> Peekyou.biz (last visited Oct. 11, 2013).
- <sup>49</sup> Singer, *supra* note 46.
- <sup>50</sup> *Id.*; Charles Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. TIMES, May 20, 2007, available at <http://www.nytimes.com/2007/05/20/business/20tele.html>.
- <sup>51</sup> Reitman, *supra* note 43.
- <sup>52</sup> Jen Wiecekner, *How the Insurer Knows You Just Stocked Up On Ice Cream and Beer*, WALL. ST. J., Feb. 25, 2013, available at <http://online.wsj.com/article/SB10001424127887323384604578326151014237898.html>.
- <sup>53</sup> *Using Fourth-Party Data Brokers to Bypass the Fourth Amendment*, SLASHDOT, Jan. 2, 2010, <http://yro.slashdot.org/story/10/01/02/0247236/using-fourth-party-data-brokers-to-bypass-the-fourth-amendment> citing Joshua L. Simmons, *Buying You: The Government's Use of Fourth-Parties to Launder Data about 'The People'*, 3 COLUM. BUS. L. REV. 950 (2009), available at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1475524](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1475524).
- <sup>54</sup> Kurt Opsahl & Rainey Reitman, *The Disconcerting Details: How Facebook Teams Up With Data Brokers to Show You Targeted Ads*, ELECTRONIC FRONTIER FOUNDATION, Apr. 22, 2013, <https://www EFF.org/deeplinks/2013/04/disconcerting-details-how-facebook-teams-up-with-data-brokers-to-show-you-targeted-ads>; Bruce Schneier, *Do You Want the Government Buying Your Data From Corporations?*, THE ATLANTIC, Apr. 30, 2013, available at <http://www.theatlantic.com/technology/archive/2013/04/do-you-want-the-government-buying-your-data-from-corporations/275431/>.
- <sup>55</sup> See Press Release, Office of Congressman Ed Markey, Lawmakers Release Information About How Data Brokers Handle Consumers' Personal Information (Nov. 8, 2012), available at <http://markey.house.gov/press-release/lawmakers-release-information-about-how-data-brokers-handle-consumers-personal>; Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA, Mar. 7, 2013, available at <https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>.
- <sup>56</sup> Julie Brill, FTC Commissioner, Federal Trade Commission, Keynote Address at the 23<sup>rd</sup> Computers Freedom and Privacy Conference (Jun. 26, 2013), available at <http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf>.
- <sup>57</sup> Duhigg, *supra* note 50.
- <sup>58</sup> Jordan Robertson, AP IMPACT: When your criminal past isn't yours, YAHOO! FINANCE, Dec. 16, 2011, <http://finance.yahoo.com/news/ap-impact-criminal-past-isnt-182335059.html>.
- <sup>59</sup> Holden Lewis, *Consumers suing to correct bad credit reports*, BANKRATE.COM, Aug. 20, 1999, <http://www.bankrate.com/bnm/news/special/19990820.asp>.
- <sup>60</sup> Edward Wyatt, *U.S. Penalizes Online Company in Sale of Personal Data*, N.Y. TIMES, June 12, 2012, at B2, available at [http://www.nytimes.com/2012/06/13/technology/ftc-leaves-first-fine-over-internet-data.html?\\_r=0](http://www.nytimes.com/2012/06/13/technology/ftc-leaves-first-fine-over-internet-data.html?_r=0).
- <sup>61</sup> Natasha Singer, *When Your Data Wanders to Places You've Never Been*, N.Y. TIMES, Apr. 27, 2013, available at <http://www.nytimes.com/2013/04/28/technology/personal-data-takes-a-winding-path-into-marketers-hands.html>.
- <sup>62</sup> Jennifer Valentino-Devries & Jeremy Singer-Vine, *They Know What You're Shopping For*, WALL. ST. J., Dec. 7, 2012, available at <http://online.wsj.com/article/SB100014241278873247844054578143144132736214.html>.
- <sup>63</sup> Lauren Drell, *4 Ways Behavioral Advertising is Changing the Web*, MASHABLE, Apr. 26, 2011, <http://mashable.com/2011/04/26/behavioral-targeting/>; Adam Tanner, *The Web Cookie is Dying. Here's The Creepier Technology That Comes Next*, FORBES.COM, June 17, 2013, <http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/>.
- <sup>64</sup> Julia Angwin, *The Web's New Goldmine: Your Secrets*, WALL. ST. J., July 30, 2010, available at <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>.
- <sup>65</sup> Emily Steel & Julia Angwin, *The Web's Cutting Edge, Anonymity in Name Only*, WALL. ST. J., Aug. 3, 2010, available at <http://online.wsj.com/article/SB10001424052748703294904575385532109190198.html?>
- <sup>66</sup> Claire Cain Miller & Somini Sengupta, *Selling Secrets of Phone Users to Advertisers*, N.Y. TIMES, Oct. 5, 2013, at A1, available at <http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html>.
- <sup>67</sup> Press Release, Network Advertising Initiative, Study Finds Behaviorally-Targeted Ads More Than Twice As Valuable, Twice As Effective As Non-Targeted Online Ads, available at [http://www.networkadvertising.org/pdfs/NAI\\_Beales\\_Release.pdf](http://www.networkadvertising.org/pdfs/NAI_Beales_Release.pdf).
- <sup>68</sup> Natasha Singer, *Your Online Attention, Bought in an Instant*, N.Y. TIMES, Nov. 17, 2012, available at <http://www.nytimes.com/2012/11/18/technology/your-online-attention-bought-in-an-instant-by-advertisers.html>; Julia Angwin, *The Web's New Goldmine: Your Secrets*, WALL. ST. J., July 30, 2010, available at <http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html>.
- <sup>69</sup> Steel & Julia Angwin, *supra* note 65; see Singer, *supra* note 68; Angwin, *supra* note 64.
- <sup>70</sup> Angwin, *supra* note 64.
- <sup>71</sup> KRISTEN PURCELL, JOANNA BRENNER, & LEE RAINIE, SEARCH ENGINE USE 2012: SUMMARY OF FINDINGS (Pew Internet & American Life Project, Mar. 9, 2012), available at <http://pewinternet.org/Reports/2012/Search-Engine-Use-2012/Summary-of-findings.aspx>.
- <sup>72</sup> See TUROW ET AL., *supra* note 4, at 3.
- <sup>73</sup> See Rainey Reitman, *A Deep Dive into Facebook and Datalogix: What's Actually Getting Shared and How to Opt-Out*, ELECTRONIC FRONTIER FOUNDATION, Sept. 25, 2012, <https://www EFF.org/deeplinks/2012/09/deep-dive-facebook-and-datalogix-whats-actually-getting-shared-and-how-you-can-opt>; TUROW ET AL., *supra* note 4; see also Ozer, *supra* note 9, at 222 (citation omitted) (discussing how consumers are rejecting targeted advertising).
- <sup>74</sup> Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 19, 2012, at MM30, available at <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.
- <sup>75</sup> Natasha Singer, *When Your Data Wanders to Places You've Never Been*, N.Y. TIMES, Apr. 27, 2013, available at <http://www.nytimes.com/2013/04/28/technology/personal-data-takes-a-winding-path-into-marketers-hands.html>.
- <sup>76</sup> Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL. ST. J., Aug. 23, 2012, available at <http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html>.
- <sup>77</sup> Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES, Feb. 19, 2012, at MM30, available at <http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.
- <sup>78</sup> Singer, *supra* note 75.
- <sup>79</sup> *Id.*
- <sup>80</sup> Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL. ST. J., Aug. 23, 2012, available at <http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html>.
- <sup>81</sup> Editorial, *Frequent Flyers, Prepare to Pay More*, N.Y. TIMES, Mar. 3, 2013, available at <http://www.nytimes.com/2013/03/04/opinion/frequent-flyers-prepare-to-pay-more.html>.
- <sup>82</sup> Lori Adams, *Facebook is Using You*, N.Y. TIMES, Feb. 4, 2012, at SR7, available at <http://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html>.
- <sup>83</sup> Jennifer Valentino-Devries, Jeremy Singer-Vine & Ashkan Soltani, *Websites Vary Prices, Deals Based on Users' Information*, WALL. ST. J., Dec. 24, 2012, at A1, available at [http://online.wsj.com/article/SB1000142412788732377204578189391813881534.html?Mod=WSJ\\_article\\_recentcolumns\\_whattheyknow](http://online.wsj.com/article/SB1000142412788732377204578189391813881534.html?Mod=WSJ_article_recentcolumns_whattheyknow).
- <sup>84</sup> See Chris Anderson & Michael Wolff, *The Web is Dead. Long Live the Internet*, WIRED, Sep. 2010, available at [http://www.wired.com/magazine/2010/08/ff\\_webrip/all/1](http://www.wired.com/magazine/2010/08/ff_webrip/all/1).
- <sup>85</sup> *What They Know – Mobile*, WALL. ST. J., <http://blogs.wsj.com/wtk-mobile/>.
- <sup>86</sup> Andrew Cunningham, *Samsung and Jay-Z give the Internet a master's class in how not to make an app*, ARS TECHNICA, July 5, 2013, <http://arstechnica.com/gadgets/2013/07/samsung-and-jay-z-give-the-internet-a-masters-class-in-how-not-to-make-an-app/>.
- <sup>87</sup> 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](http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html?mod=WSJ_WhatTheyKnowPrivacy_LeftTopNews).
- <sup>88</sup> Ozer, *supra* note 9, at 270 (citing Nicole A. Ozer, Tech. and Civil Liberties Policy Dir., ACLU of N. Cal., Comments of the American Civil Liberties Union of Northern California to the Federal Trade Commission at 5–6 (Dec. 21, 2009), available at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00068.pdf>).
- <sup>89</sup> *Id.* at 263.
- <sup>90</sup> Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, See Chris Anderson & Michael Wolff, *The Web is Dead. Long Live the Internet*, WIRED, Sep. 2010, available at [http://www.wired.com/magazine/2010/08/ff\\_webrip/all/1](http://www.wired.com/magazine/2010/08/ff_webrip/all/1), Dec. 17, 2010, available at <http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html>; Press Release, Office of the Attorney General of California, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012), available at <https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>.
- <sup>91</sup> Ozer, *supra* note 9, at 266, 270 (citing Nicole A. Ozer, Tech. and Civil Liberties Policy Dir., ACLU of N. Cal., Comments of the American Civil Liberties Union of Northern California to the Federal Trade Commission at 5–6 (Dec. 21, 2009), available at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00068.pdf>).
- <sup>92</sup> Press Release, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, Office of the Attorney General of California, Feb. 22, 2012, available at <https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>.
- <sup>93</sup> *Id.*; 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>.
- <sup>94</sup> *Id.*
- <sup>95</sup> *Id.*
- <sup>96</sup> *Pandora – What They Know – Mobile*, WALL. ST. J., Dec. 17, 2010, <http://blogs.wsj.com/wtk-mobile/2010/12/17/pandora-iphone/>.
- <sup>97</sup> *MyFitnessPal – What They Know – Mobile*, WALL. ST. J., Dec. 17, 2010, <http://blogs.wsj.com/wtk-mobile/2010/12/17/myfitness-pal/>.
- <sup>98</sup> Casey Johnson, *iOS apps are more grabby with your personal data than Android apps*, ARS TECHNICA, Mar. 6, 2013, <http://arstechnica.com/apple/2013/03/ios-apps-are-more-grabby-with-your-personal-data-than-android-apps/>.
- <sup>99</sup> Claire Cain Miller & Somini Sengupta, *Selling Secrets of Phone Users to Advertisers*, N.Y. TIMES, Oct. 5, 2013, at A1, available at <http://www.nytimes.com/2013/10/06/technology/selling-secrets-of-phone-users-to-advertisers.html>.
- <sup>100</sup> Jonah Comstock, *Pew: 19 percent of smartphone users have health apps*, MOBIHEALTHNEWS, Nov. 8, 2012, <http://mobihealthnews.com/18965/pew-19-percent-of-smartphone-users-have-health-apps/>.
- <sup>101</sup> MAEVE DUGGAN & LEE RAINIE, CELL PHONE ACTIVITIES 2012 (Pew Internet & American Life Project, Nov. 25, 2012), available at <http://www.pewinternet.org/Reports/2012/Cell-Activities/Main-Findings.aspx>.
- <sup>102</sup> FEDERAL TRADE COMMISSION, MOBILE APPS FOR KIDS; DISCLOSURES STILL NOT MAKING THE GRADE 13 (2013), available at <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf> [hereinafter MOBILE APPS FOR KIDS; DISCLOSURES].
- <sup>103</sup> *Id.*

<sup>104</sup> Edward Wyatt, *F.T.C. Suggests Privacy Guidelines for Mobile Apps*, N.Y. TIMES, Feb. 1, 2013, available at <http://www.nytimes.com/2013/02/02/technology/ftc-suggests-do-not-track-feature-for-mobile-software-and-apps.html>.

<sup>105</sup> See Ponemon, *supra* note 33.

<sup>106</sup> Only six companies (19 percent) reported that it was unlikely they would be able to comply with the law.

<sup>107</sup> CAL. CIV. CODE §§ 1798.83(b)(1); (b)(1)(A)-(C).

<sup>108</sup> *Id.* at § 1798.83(b)(1)(C).

<sup>109</sup> *Id.* at § 1798.83(b)(1)(B).

<sup>110</sup> LAUREN THOMAS & CHRIS JAY HOOFNAGLE, EXPLORING INFORMATION SHARING THROUGH CALIFORNIA'S 'SHINE THE LIGHT' LAW 5 (Aug. 13, 2009), available at <http://ssrn.com/abstract=1448365> or <http://dx.doi.org/10.2139/ssrn.1448365>.

<sup>111</sup> *Id.* at 8.

<sup>112</sup> Facebook was one of the most difficult companies to contact. Their privacy link did not work and emails to fix the error were not returned. Two participants in the ACLU-NC's study sent Facebook letters through different methods and neither received a useful response. One person's email went unanswered and another person only received all the information Facebook has collected on that person, not information the company shares. Facebook's current data use policy, dated December 11, 2012, now contains a link where users may submit a Shine the Light request. See *Data Use Policy*, FACEBOOK.COM, [https://www.facebook.com/full\\_data\\_use\\_policy](https://www.facebook.com/full_data_use_policy).

<sup>113</sup> TONY DUTZIK, ELIZABETH RIDLINGTON & PEDRO MORILLAS, STILL IN THE DARK: CALIFORNIA CONSUMERS' SEARCH FOR ANSWERS ABOUT HOW COMPANIES SHARE THEIR PERSONAL INFORMATION 1 (Frontier Group and CalPIRG Education Fund, 2008), available at <http://www.frontiergroup.org/sites/default/files/reports/Still-in-the-Dark.pdf>.

<sup>114</sup> *Id.*

<sup>115</sup> THOMAS & HOOFNAGLE, *supra* note 110, at 4, 9; CHRIS JAY HOOFNAGLE & JENNIFER KING, CONSUMER INFORMATION SHARING: WHERE THE SUN STILL DON'T SHINE 10 (Samuelson Law, Technology & Public Policy Clinic, University of California-Berkeley School of Law 10, (2007) available at <http://ssrn.com/abstract=1137990>.

<sup>116</sup> CAL. CIV. CODE § 1798.83(a).

<sup>117</sup> *Id.* at § 1798.83(b)(1)(C).

<sup>118</sup> *Id.* at § 1798.84(d).

<sup>119</sup> *Id.* at § 1798.83(b)(1)(C).

<sup>120</sup> HOOFNAGLE & KING, *supra* note 115, at 10.

<sup>121</sup> ACLU OF NORTHERN CALIFORNIA FIELD ACTIVIST COMMITTEE, 2012 GRASSROOTS STUDY OF CALIFORNIA'S SHINE THE LIGHT LAW (2012) (on file with author) [hereinafter ACLU-NC STUDY].

<sup>122</sup> *Id.*

<sup>123</sup> DUTZIK, *supra* note 113, at 2.

<sup>124</sup> CAL. CIV. CODE § 1798.83(e)(2). "Direct marketing purposes" means the use of personal information to solicit or induce a purchase, rental, lease, or exchange of products, goods, property, or services directly to individuals by means of the mail, telephone, or electronic mail for their personal, family, or household purposes. The sale, rental, exchange, or lease of personal information for consideration to businesses is a direct marketing purpose of the business that sells, rents, exchanges, or obtains consideration for the personal information."

<sup>125</sup> THOMAS & HOOFNAGLE, *supra* note 110, at 6-7.

<sup>126</sup> ACLU-NC STUDY, *supra* note 121.

<sup>127</sup> This includes Yelp, Twitter, Verizon, Yahoo!, LinkedIn, and Apple. See *Privacy Policy*, YELP!, (policy last updated Nov. 27, 2012), [http://www.yelp.com/static?country\\_US&p=privacy](http://www.yelp.com/static?country_US&p=privacy); *Cookies on the LinkedIn site*, LINKEDIN, Sept. 26, 2012, <http://www.linkedin.com/legal/cookie-policy>; *Privacy Policy*, VERIZON, <http://www22.verizon.com/about/privacy/policy/> (policy last updated March 2013); *Yahoo! Privacy Policy*, YAHOO!, (policy last updated May 31, 2013), <http://info.yahoo.com/privacy/us/yahoo/details.html#4>; *Privacy Policy*, APPLE, (policy last updated Aug. 1, 2013), <https://www.apple.com/privacy/>; *Twitter Privacy Policy*, TWITTER, <https://twitter.com/privacy> (policy last updated July 3, 2013).

<sup>128</sup> *Privacy Policy*, VERIZON, <http://www22.verizon.com/about/privacy/policy/> (policy last updated March 2013) ("We also share certain types of customer information within our family of companies for our own marketing purposes unless you advise us not to share."); *Yahoo! Privacy Policy*, YAHOO!, (policy last updated May 31, 2013), <http://info.yahoo.com/privacy/us/yahoo/details.html#4> ("We provide the information to trusted partners ... These companies may use your personal information to help Yahoo! communicate with you about offers from Yahoo! and our marketing partners."); *Privacy Policy*, APPLE, (policy last updated Aug. 1, 2013), <https://www.apple.com/privacy/> ("At times Apple may make certain personal information available to strategic partners ... that help Apple market to customers.").

<sup>129</sup> CAL. CIV. CODE § 1798.83(c)(2).

<sup>130</sup> HOOFNAGLE & KING, *supra* note 115, at 10.

<sup>131</sup> THOMAS & HOOFNAGLE, *supra* note 110, at 7-8.

<sup>132</sup> ACLU-NC STUDY, *supra* note 121.

<sup>133</sup> See Christine Jolls, *Privacy and Consent Over Time: The Role of Agreement in Fourth Amendment Analysis*, 54 WILLIAM & MARY L. REV. 1693 (2013), available at <http://wmlawreview.org/files/10-Jolls.pdf> (comparing employee time-of-hire consent agreements to random drug tests to time-of-hire consent agreements to random computer searches, examining modern behavioral economics research, and concluding as a general matter that it is inappropriate to equate contemporaneous and in-advance express search agreements because people have an irrational understanding of how the latter may affect their privacy going forward).

<sup>134</sup> CAL. CIV. CODE § 1798.83(e)(6)(A) (including, *inter alia*, "Names of children," "Electronic mail or other addresses of children," "Political party affiliation," and "Social security number").

<sup>135</sup> Dana Hull, *New From PPIIC: 58 Percent Of Californians Have A Smart Phone*, SILICONBEAT, Jun. 26, 2013, <http://www.siliconbeat.com/2013/06/26/new-from-ppic-58-percent-of-californians-have-a-smart-phone/>.

<sup>136</sup> Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL. ST. J., Aug. 4, 2010, available at <http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html>. In 2010, an Arizona resident activated the GPS of his wife's phone without her knowledge and used it to stalk and find her and then kill her and their two children. In 2011, a Washington mechanic used the GPS signal from his wife's phone to find and kill her and their five children.

<sup>137</sup> 19 percent of smartphone users have apps for health purposes. 35 percent of U.S. adults also use the Internet to look for health information. Susannah Fox & Maeve Duggan, MOBILE HEALTH 2012, (Pew Internet & American Life Project, Nov. 8, 2012) available at <http://pewinternet.org/Reports/2012/Mobile-Health.aspx>; SUSANNAH FOX & MAEVE DUGGAN, HEALTH ONLINE 2013 (Pew Internet & American Life Project, Jan. 15, 2013), available at [http://www.pewinternet.org/~media/Files/Reports/2013/Pew Internet Health Online report.pdf](http://www.pewinternet.org/~media/Files/Reports/2013/Pew%20Internet%20Health%20Online%20report.pdf).

<sup>138</sup> Valentino-Devries & Singer-Vine, *supra* note 62.

<sup>139</sup> Rainey Reitman, *Six Heartbreaking Truths about Online Dating Privacy*, ELECTRONIC FRONTIER FOUNDATION, Feb. 10, 2012, available at <https://www EFF.org/deeplinks/2012/02/six-heartbreaking-truths-about-online-dating-privacy>, citing <http://cyberlaw.stanford.edu/node/6740>.

<sup>140</sup> CAL. CIV. CODE § 1798.83(e)(8); see also FTC PRIVACY RECOMMENDATIONS, *supra* note 19, at 41-42.

<sup>141</sup> HOOFNAGLE & KING, *supra* note 115, at 16; THOMAS & HOOFNAGLE, *supra* note 110, at 7.

<sup>142</sup> THOMAS & HOOFNAGLE, *supra* note 110, at 7.

<sup>143</sup> ACLU-NC STUDY, *supra* note 121; *Privacy Policy*, VERIZON, <http://www22.verizon.com/about/privacy/policy/> (policy last updated March 2013) ("We also share certain types of customer information within our family of companies for our own marketing purposes unless you advise us not to share.").

<sup>144</sup> CAL. CIV. CODE § 1798.83(e)(5).

<sup>145</sup> Angwin, *supra* note 64.

<sup>146</sup> *Id.*; Arvind Narayanan, *Do Not Track Isn't Just About Behavioral Advertising*, CENT. STANFORD CENTER FOR INTERNET & SOCIETY (Dec. 20, 2010), <http://http://cyberlaw.stanford.edu/node/6573>.

<sup>147</sup> HOOFNAGLE & KING, *supra* note 115, at 11.

<sup>148</sup> THOMAS & HOOFNAGLE, *supra* note 110, at 8.

<sup>149</sup> *Id.* at 4, 9.

<sup>150</sup> Press Release, Office of the Attorney General of California, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012), available at <https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>.

<sup>151</sup> Rachelle Chong, *California Assembly Select Committee on Privacy Holds Hearing*, TECHWIRE.NET, Mar. 19, 2013, <http://techwire.net/california-assembly-select-committee-on-privacy-holds-hearing/>.

<sup>152</sup> In 2013, California lawmakers introduced several privacy bills aimed at increasing transparency. Amongst these bills is the Right to Know Act (Lowenthal), a bill that would update and expand the transparency right first introduced with Shine the Light. A.B. 1291, 2013-2014 Leg., Reg. Sess. (Cal. 2013), available at [http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab\\_1251-1300/ab\\_1291\\_bill\\_20130401\\_amended\\_asm\\_v98.htm](http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_1251-1300/ab_1291_bill_20130401_amended_asm_v98.htm). Another landmark bill would require the government get a warrant to access emails and requires account owners be told it happens. S.B. 467, 2013-2014 Leg., Reg. Sess. (Cal. 2013), available at [http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb\\_0451-0500/sb\\_467\\_bill\\_20130401\\_amended\\_sen\\_v98.htm](http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0451-0500/sb_467_bill_20130401_amended_sen_v98.htm). One other measure would limit websites' collection of minors' personal information without clear parental notice. A.B. 319, 2013-2014 Leg., Reg. Sess. (Cal. 2013), available at [http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab\\_0301-0350/ab\\_319\\_bill\\_20130212\\_introduced.html](http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0301-0350/ab_319_bill_20130212_introduced.html). A now-enacted bill will require that websites disclose the presence of third party trackers and state whether they comply with Do Not Track. A.B. 370, 2013-2014 Leg., Reg. Sess. (Cal. 2013), available at [http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab\\_0201-0250/ab\\_370\\_bill\\_20130206\\_introduced.html](http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0201-0250/ab_370_bill_20130206_introduced.html). Finally, a set of bills would also amend the California Online Privacy Protection Act, explicitly extending its requirements to mobile apps and mobile advertisers all while making privacy notices more concise. A.B. 257, 2013-2014 Leg., Reg. Sess. (Cal. 2013), available at [http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab\\_0251-0300/ab\\_257\\_bill\\_20130207\\_introduced.pdf](http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0251-0300/ab_257_bill_20130207_introduced.pdf); A.B. 242, 2013-2014 Leg., Reg. Sess. (Cal. 2013), available at [http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab\\_0201-0250/ab\\_242\\_bill\\_20130206\\_introduced.html](http://www.leginfo.ca.gov/pub/13-14/bill/asm/ab_0201-0250/ab_242_bill_20130206_introduced.html).

<sup>153</sup> CAL. BUS. & PROF. CODE §§ 22575-79.

<sup>154</sup> Press Release, Office of the Attorney General of California, Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law (Oct. 30, 2012) available at <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance>.

<sup>155</sup> Facebook, Amazon, Apple, Google, Hewlett-Packard, Microsoft, and Research in Motion are parties to this agreement. See Press Release, Office of the Attorney General of California, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications (Feb. 22, 2012), available at <https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>; Press Release, Office of the Attorney General of California, Attorney General Kamala D. Harris Announces Expansion of California's Consumer Privacy Protections to Social Apps as Facebook Signs Apps Agreement (June 22, 2012), available at <http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer>.

<sup>156</sup> CALIFORNIA ATTORNEY GENERAL KAMALA D. HARRIS, CALIFORNIA DEPARTMENT OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM (Jan. 2013), available at [http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy\\_on\\_the\\_go.pdf](http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf) [hereinafter RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM].

<sup>157</sup> *Id.*

<sup>158</sup> FTC PRIVACY RECOMMENDATIONS, *supra* note 19, at I, 66.

<sup>159</sup> Brill, *supra* note 56.

<sup>160</sup> Natasha Singer, *Consumer Data, But Not For Consumers*, N.Y. TIMES, July 21, 2012, available at <http://www.nytimes.com/2012/07/22/business/axiom-consumer-data-often-unavailable-to-consumers.html>.

<sup>161</sup> See FEDERAL TRADE COMMISSION, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING (FTC Staff Report, Feb. 2012), available at [http://www.ftc.gov/os/2012/02/120216mobile\\_apps\\_kids.pdf](http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf); MOBILE APPS FOR KIDS; DISCLOSURES, *supra* note 102; Edward Wyatt, *F.T.C. Suggests Privacy Guidelines for Mobile Apps*, N.Y. TIMES, Feb. 1, 2013, available at <http://www.nytimes.com/2013/02/02/technology/ftc-suggests-do-not-track-feature-for-mobile-software-and-apps.html>.

<sup>162</sup> Ramirez, *supra* note 41.

<sup>163</sup> THE WHITE HOUSE, CONSUMER DATA PRIVACY: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 15, 19, (Feb. 2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf> [hereinafter CONSUMER PRIVACY FRAMEWORK].

<sup>164</sup> See CONSUMER PRIVACY FRAMEWORK, *supra* note 163, at 15, 19 (warning that “[a]s third parties become further removed from direct interactions with consumers, it may be more difficult for them to provide consumers with meaningful control over data collection.”); Chris Jay Hoofnagle et. al., *Behavioral Advertising: The Offer You Cannot Refuse*, 6 HARVARD L. & POL. REV. 273 (2012), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2137601](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2137601); FTC PRIVACY RECOMMENDATIONS, *supra* note 19.

<sup>165</sup> Natasha Singer, *Congress to Examine Data Sellers*, N.Y. TIMES, May 21, 2013, available at <http://www.nytimes.com/2012/07/25/technology/congress-opens-inquiry-into-data-brokers.html>.

<sup>166</sup> Bobby Caina Calvan, *Data collection companies defend their role*, BOSTON GLOBE, Nov. 8, 2012, available at <http://www.bostonglobe.com/news/politics/2012/11/08/data-collectors-reject-assertions-they-are-data-brokers-congress-looks-impose-rules/W4YavL0OVBLxv95SK7sWO/story.html>.

<sup>167</sup> Press Release, Democratic Press Office, Rockefeller Seeks Information About Data Brokers' Practices (Oct. 10, 2012), available at [http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord\\_id=a42a865a-be30-4171-8278-86ee0a8c76fb&ContentType\\_id=77eb43da-aa94-497d-a73f-5c951f72372&Group\\_id=165806cd-d931-4605-aa86-7fabc5fd3536&YearDisplay=2012](http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=a42a865a-be30-4171-8278-86ee0a8c76fb&ContentType_id=77eb43da-aa94-497d-a73f-5c951f72372&Group_id=165806cd-d931-4605-aa86-7fabc5fd3536&YearDisplay=2012); Press Release, Democratic Press Office, Rockefeller Expands Data Broker Investigation (Sept. 25, 2013) available at [http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord\\_id=0491f142-c80f-487e-81a1-7012a7592794&ContentType\\_id=77eb43da-aa94-497d-a73f-5c951f72372&Group\\_id=4b968841-f3e8-49da-a529-7b18e32fd69d](http://www.commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=0491f142-c80f-487e-81a1-7012a7592794&ContentType_id=77eb43da-aa94-497d-a73f-5c951f72372&Group_id=4b968841-f3e8-49da-a529-7b18e32fd69d).

<sup>168</sup> Somini Sengupta, *Senator Asks Cellphone Carriers: What Exactly Do You Share With Government?*, N.Y. TIMES, [http://bits.blogs.nytimes.com/2013/09/12/senator-asks-cellphone-carriers-what-exactly-do-you-share-with-government/?\\_r=0](http://bits.blogs.nytimes.com/2013/09/12/senator-asks-cellphone-carriers-what-exactly-do-you-share-with-government/?_r=0).

<sup>169</sup> CONSUMER PRIVACY FRAMEWORK, *supra* note 163, at 15, 19.

<sup>170</sup> *Id.*

<sup>171</sup> Ina Fried, *EU Commissioner: We Don't Want U.S. Reading Our Mail and Listening to Our Phone Calls*, ALL THINGS DIGITAL, July 15, 2013, <http://allthingsd.com/20130715/eu-commissioner-we-dont-want-u-s-reading-our-mail-and-listening-to-our-phone-calls/>.

<sup>172</sup> Donald C. Dowling, Jr., *International Data Protection and Privacy Law*, WHITE & CASE, (Aug. 2009), at 26, [http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5dfd2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article\\_IntlDataProtectionandPrivacyLaw\\_v5.pdf](http://www.whitecase.com/files/Publication/367982f8-6dc9-478e-ab2f-5dfd2d96f84a/Presentation/PublicationAttachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_IntlDataProtectionandPrivacyLaw_v5.pdf); *Leading by Example: Key Developments in the First Seven Years of PIPEDA*, GOV. OF CANADA, [http://www.priv.gc.ca/information/pub/lbe\\_080523\\_e.asp#conclusion](http://www.priv.gc.ca/information/pub/lbe_080523_e.asp#conclusion).

<sup>173</sup> Sam Pfeifle, *Stoddart: PIPEDA Needs Reform To Bring Enforcement Powers*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, May 23, 2013, available at [https://www.privacyassociation.org/publications/2013\\_05\\_22\\_stoddart\\_pipeda\\_needs\\_reform\\_to\\_bring\\_enforcement\\_powers?utm\\_source=Facebook&utm\\_medium=05-24-13&utm\\_campaign=DD](https://www.privacyassociation.org/publications/2013_05_22_stoddart_pipeda_needs_reform_to_bring_enforcement_powers?utm_source=Facebook&utm_medium=05-24-13&utm_campaign=DD).

<sup>174</sup> Shane Schick, *Jennifer Stoddart: Canada's best privacy commissioner?*, YAHOO! FINANCE CANADA, Mar. 1, 2013, <http://ca.finance.yahoo.com/blogs/dashboard/jennifer-stoddart-canada-best-privacy-commissioner-161627989.html>.

<sup>175</sup> Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection Of Individuals With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data. 1995 O.J. (L 281/31), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML> [hereinafter “EU Directive”].

<sup>176</sup> See *id.* at art. 12(a) (which “guarantee[s] every data subject the right to obtain ... without constraint at reasonable intervals and without excessive delay or expense... the recipients or categories of recipients to whom the data are disclosed....”).

<sup>177</sup> Opinion 4/2007, Article 29 Data Protection Working Party, Jun. 20, 2007, at 16-17, available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf); see also OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, REPORT ON THE 2010 OFFICE OF THE PRIVACY COMMISSIONER OF CANADA'S CONSULTATIONS ON ONLINE TRACKING, PROFILING AND TARGETING, AND CLOUD COMPUTING, available at [https://webcache.googleusercontent.com/search?q=cache:https://www.priv.gc.ca/resource/consultations/report\\_201105\\_e.asp](https://webcache.googleusercontent.com/search?q=cache:https://www.priv.gc.ca/resource/consultations/report_201105_e.asp) (interpreting Canada's privacy laws and stating that “[t]he Office [of the Privacy Commissioner of Canada] has also determined that an IP address is personal information if it can be associated with an identifiable individual.”).

<sup>178</sup> DOUWE KORFF, EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE: COMPARATIVE SUMMARY OF NATIONAL LAWS 103 (University of Essex, Sept. 2002), available at <http://www.garantepriacy.it/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE>.

<sup>179</sup> European Commission General Data Protection Regulation, COM (2012) 11 final, available at [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf); see also *Why do we need an EU data protection reform?*, EUROPEAN COMMISSION, [http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf).

<sup>180</sup> *Accessing Your Facebook Info*, FACEBOOK.COM, <https://www.facebook.com/help/405183566203254> (last visited Sept. 19, 2013).

<sup>181</sup> *Google Takeout*, GOOGLE, <https://www.google.com/takeout/?pli=1> (last visited Sept. 19, 2013).

<sup>182</sup> Mika Raento, *The Data Subject's Right of Access and to be Informed in Finland: An Experimental Study*, 3 INT'L J. OF L. AND INFO. TECH. 390, 398 (Vol. 14 2006), available at <http://ssrn.com/abstract=1098660> or <http://dx.doi.org/10.1093/ijit/ea1008>.

<sup>183</sup> *Id.* at 401.

<sup>184</sup> KORFF, *supra* note 178, at 103.

<sup>185</sup> Ozer, *supra* note 9; Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, Feb. 7, 2012, FORBES.COM, <http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/>.

<sup>186</sup> Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, March 26, 2011, available at <http://www.nytimes.com/2011/03/26/business/media/26privacy.html>.

<sup>187</sup> *Id.*

<sup>188</sup> Natasha Singer, *If My Data is An Open Book, Why Can't I Read It*, N.Y. TIMES, May 25, 2013, available at <http://www.nytimes.com/2013/05/26/technology/for-consumers-an-open-data-society-is-a-misnomer.html?src=recg>; Nicole Ozer, *PRISM: Bringing The Need for Better Transparency and Privacy Into Focus*, ACLU-NC BYTES AND PIECES BLOG, Jul. 2, 2013, [https://www.aclunc.org/issues/technology/blog/prism\\_bringing\\_the\\_need\\_for\\_better\\_transparency\\_and\\_privacy\\_into\\_focus.shtml](https://www.aclunc.org/issues/technology/blog/prism_bringing_the_need_for_better_transparency_and_privacy_into_focus.shtml).

<sup>189</sup> *Google Takeout*, GOOGLE, <https://www.google.com/takeout/?pli=1> (last visited Sept. 19, 2013).

<sup>190</sup> Leslie Horn, *Here's How to Download All Your Tweets*, GIZMODO, Dec. 19, 2012, <http://gizmodo.com/5969755/heres-how-to-download-all-your-tweets-ever>.

<sup>191</sup> Kevin Chen, *LinkedIn Updates Privacy Policy to Let In Advertisers*, THE MOTLEY FOOL, May 11, 2013, <http://www.fool.com/investing/general/2013/05/11/linkedin-updates-privacy-policy-to-let-in-advertisers.aspx>.

<sup>192</sup> Natasha Singer, *Axiom Lets Consumer See Data It Collects*, N.Y. TIMES, Sept. 4, 2013, available at [http://www.nytimes.com/2013/09/05/technology/axiom-lets-consumers-see-data-it-collects.html?pagewanted=all&\\_r=0](http://www.nytimes.com/2013/09/05/technology/axiom-lets-consumers-see-data-it-collects.html?pagewanted=all&_r=0).

<sup>193</sup> *Amazon Advertising Preferences*, AMAZON.COM, <http://www.amazon.com/gp/dra/info> (last visited Sept. 19, 2013); *Google Ads Settings*, GOOGLE.COM, [www.google.com/settings/ads](http://www.google.com/settings/ads); *Ad Interest Manager*, YAHOO!, [http://info.yahoo.com/privacy/us/yahoo/opt\\_out/targeting/](http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting/) (last visited Sept. 19, 2013).

<sup>194</sup> Mark Zuckerberg, *Our Commitment to the Facebook Community*, THE FACEBOOK BLOG, Nov. 29, 2011, <https://blog.facebook.com/blog.php?post=10150378701937131>.

<sup>195</sup> The new rules of the game: Conference on technology and privacy, 34<sup>th</sup> International Conference of Data Protection and Privacy Commissioner, <http://privacyconference2012.org/english/sobre-la-conferencia/noticias/Las-nuevas-reglas-del-juego-conferencia-sobre-tecnologia-y-privacidad>.

<sup>196</sup> Google Transparency Report, GOOGLE, <http://www.google.com/transparencyreport/> (last visited October 15, 2013).

<sup>197</sup> Jeremy K., *Twitter Transparency Report*, TWITTER BLOG, July 2, 2012, <https://blog.twitter.com/2012/twitter-transparency-report>; *Transparency Report*, DROPBOX, <https://www.dropbox.com/transparency> (report last updated January 31, 2013); Brad Smith, *Microsoft Releases 2012 Law Enforcement Requests Report*, MICROSOFT ON THE ISSUES, Mar. 21, 2013, [https://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2013/03/20/microsoft-releases-2012-law-enforcement-requests-report.aspx?Redirected=true](https://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/03/20/microsoft-releases-2012-law-enforcement-requests-report.aspx?Redirected=true).

<sup>198</sup> Glenn Greenwald & Ewen MacAskill, *NSA Prism programs taps into user data of Apple, Google and others*, THE GUARDIAN, June 6, 2013, available at <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

<sup>199</sup> See Marisa Mayer & Ron Bell, *Our Commitment to Our Users' Privacy*, YAHOO!, Jun. 17, 2013, <http://yahoo.tumblr.com/post/53243441454/our-commitment-to-our-users-privacy>; Ted Lilloyt, *Facebook Releases Data, Including All National Security Requests*, FACEBOOK NEWSROOM, Jun. 14, 2013, <https://newsroom.fb.com/News/636/Facebook-Releases-Data-Including-All-National-Security-Requests>; Apple's Commitment to Customer Privacy, APPLE.COM, Jun. 16, 2013, <https://www.apple.com/apples-commitment-to-customer-privacy/>.

<sup>200</sup> Colin Stretch, *Global Government Requests Report*, FACEBOOK NEWSROOM, Aug. 27, 2013, <https://newsroom.fb.com/News/699/Global-Government-Requests-Report>; Ron Bell, *Sharing Our First Transparency Report*, Sept. 6, 2013, available at <http://yahoo.tumblr.com/post/60456292987/sharing-our-first-transparency-report>.

<sup>201</sup> See CONSUMER PRIVACY FRAMEWORK, *supra* note 163, at 1; FTC PRIVACY RECOMMENDATIONS, *supra* note 19 at iv; RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM, *supra* note 156, at 9.

<sup>202</sup> See, e.g., *Google Takeout*, GOOGLE, <https://www.google.com/takeout/?pli=1> (last visited Sept. 19, 2013); *Accessing Your Facebook Info*, FACEBOOK.COM, <https://www.facebook.com/help/405183566203254> (last visited Sept. 19, 2013).

<sup>203</sup> See CAL. CIVIL CODE §1798.80(e) (defining personal information to include any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.”).

<sup>204</sup> FTC PRIVACY RECOMMENDATIONS, *supra* note 19, at 15.

<sup>205</sup> *Id.*

<sup>206</sup> *Id.* at 41-42.

<sup>207</sup> William K. Darley & Jeen-Su Lim, *PERSONAL RELEVANCE AS MODERATOR OF THE EFFECT OF PUBLIC SERVICE ADVERTISING ON BEHAVIOR*, ADVANCES IN CONSUMER RESEARCH Volume 18, 1991, available at <http://www.acrwebsite.org/search/view-conference-proceedings.aspx?ld=7177>.





**Read a book  
about cancer**

**Like vodka**

**Studying  
Arabic**

**“The time has come for businesses  
to move their data collection and  
use practices out of the shadows  
and into the sunlight.”**

**–FTC Chairwoman Edith Ramirez**



Online at [www.aclunc.org/R2K](http://www.aclunc.org/R2K)