SB 118

<TARGET><BILL>SB 118</BILL><SUBJECT>SB 118</SUBJECT><COMM></COMM></TARGET>

ALASKA STATE LEGISLATURE

Session
State Capitol, Rm. 7
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

Interim
1500 W. Benson Blvd. #218
(907) 269-0120
Fax: (907) 269-0122

Sen.Bill.Wielechowski@legis.state.ak.us

Resources Committee

Joint Armed Services Committee

Judiciary Committee

SENATOR BILL WIELECHOWSKI

MEMORANDUM

DATE: 29 March 2018

TO: Senator Kevin Meyer
Chair, Senate State Affairs Committee

FROM: Senator Bill Wielechowski

SUBJ: Hearing Request for SB 118

Dear Chair Meyer,

I respectfully request a hearing for SB 118 in the Senate State Affairs Committee. SB 118 is a bill that, if approved, would protect the privacy of Alaskans through increasing transparency and establishing standards for businesses that collect and disclose personal digital information.

Please find the following documents attached to this request:

- SB 118 Version A
- SB 118 Sponsor Statement
- SB 118 Sectional Analysis
- SB 118 Supporting Document- Americans and Cybersecurity- Pew Research Center
- SB 118 Supporting Document- Data Brokers: Companies Are Buying, Sharing Your Online Info- NPR, All Tech Considered
- SB 118 Supporting Document- Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns- Journal of Business Ethics
- SB 118 Supporting Document- Right to Know Act- ACLU of Northern California
- SB 118 Supporting Document- Hey That's Personal: When Companies Sell Customer Information Gathered Through the Internet - American Bar Association Business Section

SB 118 Disclosure of Customer Information
Senator Wielechowski

What this bill does

Also known as the "Right to Know Act" this bill would require owners of internet and online services to keep individual customers personal information private. The would need to 1) identify categories of personal information that the owner collects about the customer, 2) identify all the third parties to whom the owner discloses, or may disclose that the owner collects through an internet website or online service, 3) describe a customer's right and 4) provide a request address, email or toll-free number that the customer can use to request or obtain the information the owner is required to provide.

Additionally, this bill would require that an owner that discloses a customer's personal information to a third party must upon request and without charge provide who the owner discloses to.

The bill further details what can be construed as personal information: name, alias, nickname, username, postal address, email, telephone no., financial accounts, government identification numbers, date of birth, age, physical characteristics, sexual information, gender, race, ethnicity, religious affiliation or activity, political affiliation or activity, professional or employment-related information, educational information, medical information, financial information, commercial information (records of property, etc.), location, internet protocol addresses, mobile phone activity, any customer generated content, or children related to the customer.

There are some exemptions and customers may recover $5,000 or actual damages, whichever is greater.

Potential Issues:

While I understand that there is a lot of concern about internet privacy right now and I can see how this bill would simply be added to the list of things that one agrees to when engaging in internet commerce through a user agreement whether it be a phone app, a website that sells stuff, etc. I don't know if this will be effective. It is unclear exactly what the "Right of Action" entails in terms of

how the customer who is subject of the violation recovers from the owner $5,000 in damages or more. This would be like you checking with all the internet providers and websites you shop on to see if they have shared your information and if they have then going to court. It is impractical to carry out, the genie is out of the bottle in terms of interstate commerce via the internet. Companies that TRY to keep your information private have data breeches all the time—banks, hospitals, etc. However, with the requirement of the companies to disclose and the right of a person to object and keep their information private—at least there is a way to get damages.

Legislative History

There has been some discussion in other states about this right to privacy on the internet or right to know, but I don't know much other than a cursory google search. I would have to ask Leg Research or NCSL look a little further afield to tell me more.

QUESTIONS:

- I see that this bill has been modeled after "Right to Know" legislation but I am curious, was there any discussion on using the California "Shine the Light" legislation as a model?

- Is there legislation on the national level that attempts to address this privacy issue? It would seem that it would take time to do this state by state but if there were a national law it may be more enforceable.

- So under this legislation, anyone who does business on the internet would have to keep records of all transactions and then if a customer decides it wants to know if their information has been sold to a third party the business has to provide the information of who they sold the customer's information to? Could you walk me through how this would work?

ALASKA STATE LEGISLATURE

Session

State Capitol, Rm. 7
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

Interim

1500 W. Benson Blvd Suite 228
Anchorage, AK 99503
(907) 269-0120
Fax: (907) 269-0122

Senator.Bill.Wielechowski@akleg.gov

Resources Committee

Joint Armed Services Committee

Judiciary Committee

SENATOR BILL WIELECHOWSKI

Sponsor Statement SB 118

An Act Relating to the Disclosure of Personal Information,

"Right to Know Act"

Alaskans have a constitutional right to privacy and this right is being infringed upon daily as Alaskans use the Internet. A multitude of commercial websites and online services collect, share, and sell the personal information of Internet users. The Right to Know Act will protect the privacy of Alaskans through increasing transparency and establishing standards for businesses that collect or disclose personal digital information.

Personal digital data is an extremely valuable commodity in the modern marketplace. It is often referred to as "a digital gold mine" and major revenues are brought in by companies who trade in this digital information. Digital data is analyzed by data brokerage companies and used to categorize consumers and target marketing.

Consumers are often unaware that their personal data is collected and may not agree with this data being held, stored or sold. Individuals are deeply concerned about the security of their personal data and, according to a study by the Pew Research Center, "Roughly half of Americans do not trust the federal government or social media sites to protect their data."

Alaskans deserve to feel secure about their private information online and should have access to the types of information collected about them and how it is used.

Sensitive digital information related to a person's identity, health, beliefs, finances or personal preferences must be kept safe. There is currently no law that adequately addresses the issue of personal data security and very little oversight regarding how Internet companies can use this information. Timely legislation addressing this topic is essential since attempts at industry self-regulation and regulation by third parties have been largely unsuccessful and the data collection industry is rapidly expanding. When Alaskans become better informed of how protective of customer privacy a business is, they can make clear choices based on how a business collects and handles their personal information. SB 118 will protect Alaskans' rights and provide our citizens with the tools they need to make informed decisions about their Internet use.

ALASKA STATE LEGISLATURE

Session

State Capitol, Rm. 7
Juneau, AK 99801
(907) 465-2435
Fax: (907) 465-6615

Interim

716 W. 4th Ave, Ste. 409
Anchorage, AK 99501
(907) 269-0120
Fax: (907) 269-0122

Senator.Bill.Wielechowski@akleg.gov

Resources Committee

State Affairs Committee

Joint Armed Services Committee

Judiciary Committee

SENATOR BILL WIELECHOWSKI

SECTIONAL ANALYSIS
Senate Bill 118
An Act Relating to the Disclosure of Personal Information,

"Right to Know Act"

Section 1: Titles this legislation the "Right to Know Act."

Section 2: Enumerates legislative findings relating to Alaska's constitutional right to privacy, the importance of transparency and security for consumers, and business practices relating to personal digital data.

Section 3: **Sec. 45.48.800-** Requires the owner of a commercial Internet website or commercial online service to notify customers of their information sharing practices. Outlines what information the owner must include in the notification.

Sec. 45.48.810- Requires the owner of a commercial Internet website or commercial online service, if requested by the customer, to provide the customer any information shared about them in the previous 12 months. Outlines which information the owner must provide.

Sec. 45.48.820- Identifies the categories of personal information to be used by the owner.

Sec. 45.48.830- Outlines exemptions from the disclosure requirements.

Sec. 45.48.840- Allows the customer to recover damages from of the owner of a commercial Internet website or commercial online service for violation of the "Right to Know Act".

Sec. 45.48.850- Outlines how the "Right to Know Act" interacts with existing law.

Sec. 45.48.890- Provides definitions.

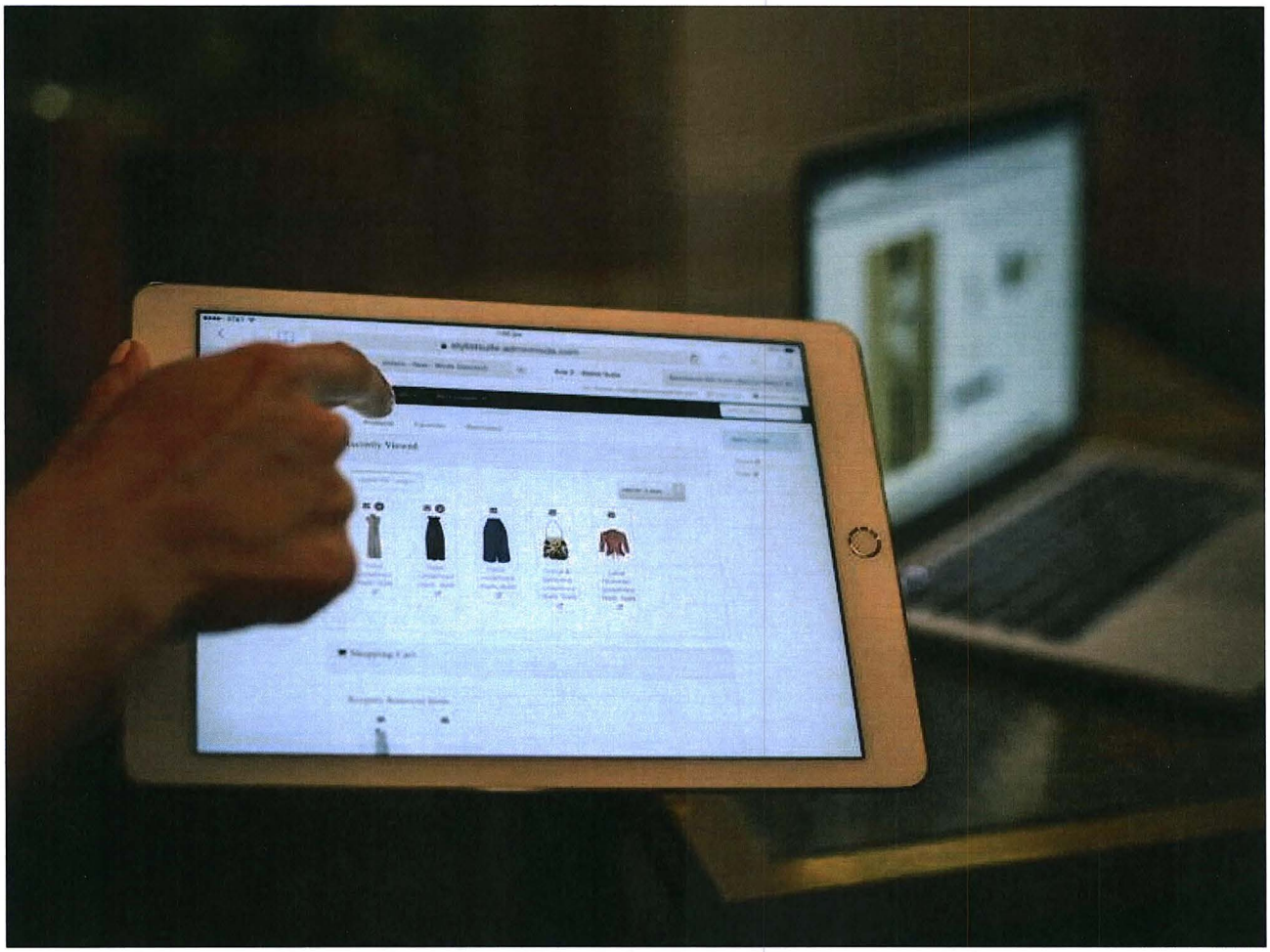
Section 4: Establishes that the "Right to Know" act is only applicable to data collected after its effective date.

THE INDUSTRY

Firms Are Buying, Sharing Your Online Info. What Can You Do About It?

July 11, 2016 · 4:51 PM ET
Heard on All Things Considered

BRIAN NAYLOR



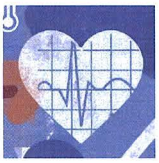
Data brokers collect information on how you use the Internet, from personal data you share on Facebook to online shopping.

Bloomberg via Getty Images

There are some big companies out there that you've probably never heard of, that know more about you than you can imagine.

They're called data brokers, and they collect all sorts of information — names, addresses, income, where you go on the Internet and who you connect with online. That information is then sold to other companies. There are few regulations governing these brokers.

Data brokers have been around for a long time, collecting information about your magazine and newspaper subscriptions. They know whether you prefer dogs or cats. From public records they can tell if you drive a Ford or a Subaru or if you've declared bankruptcy.



ALL TECH CONSIDERED

Online Health Searches Aren't Always Confidential

But the Internet upped the ante considerably. Think of all that personal data you share on Facebook, or your online shopping. According to Julie Brill, who recently stepped down as a commissioner on the Federal Trade Commission, these companies share just about everything.

"It's what Web pages we visit, where we're shopping, who we're interfacing with on social media — all of that information is available to be collected by entities that park themselves on the various websites," Brill said.

Once these companies collect the information, the data brokers package and sell it — sometimes to other brokers, sometimes to businesses — that then use the information to target ads to consumers. And it's a lucrative industry. One of the largest brokers, Acxiom, reported over $800 million in revenue last year.

When the FTC studied data brokers two years ago, it found that brokers take the information they gleaned about consumers and use it to put us into categories.

Some of the categories are innocuous — pet owner, or winter sports enthusiast.

ALL TECH CONSIDERED

This Week In Data Collection News, And The Privacy Paradox

But Brill says others were more problematic, like "single mom struggling in an urban setting" or "people who did not speak English and felt more comfortable speaking in Spanish" or "gamblers."

"And so the concern is not only the fact that these profiles are being created, but how are they being used," Brill said.

Say, for instance, you do an online search for heart disease or diabetes.

Depending upon the website, that information can go to ad networks and analytics companies. If the contents of that heart disease or diabetes search end up with a data broker, that information could then be added to your digital biography.

"That becomes a part of your profile and others see that and can market to you based on that information," Brill said.

ALL TECH CONSIDERED

A Closer Look At Obama's Plan To Protect Consumer Data

And there's little to stop data brokers from using the information they've gathered from us in whatever way they please, says Jeff Chester, a privacy advocate and director of the Center for Digital Democracy.

"Because there are no online privacy laws in the United States, there's no stop sign, there's no go slow sign, there's no crossing guard. The message is anything goes," Chester said.

Like Chester, former FTC Commissioner Brill says legislation is needed to make the industry more transparent.

She says there should be a website where consumers could see what data has been collected about them and correct it or block it from being used. Some individual companies, like Acxiom, do this.

And the industry does have voluntary guidelines to limit how information is used.

Xenia Boone is the vice president for corporate and social responsibility at the Direct Marketing Association, which represents many data brokers. She says companies are not creating "dossiers" about consumers.

ALL TECH CONSIDERED

If There's Privacy In The Digital Age, It Has A New Definition

Boone says marketing companies and fundraiser organizations "are working with data companies in order to get the right information about potential prospects because they need to go out there, they need the data in order to reach someone."

A marketing industry website, aboutads.info, lets consumers opt out of having some ads sent to their browsers. Consumers can also block individual ads by clicking on that little triangle in the upper right hand corner of many of them. You can also install an ad blocker and clear the cookies from your browser.

But blocking ads is one thing, keeping your information away from the data brokers is much harder to do.

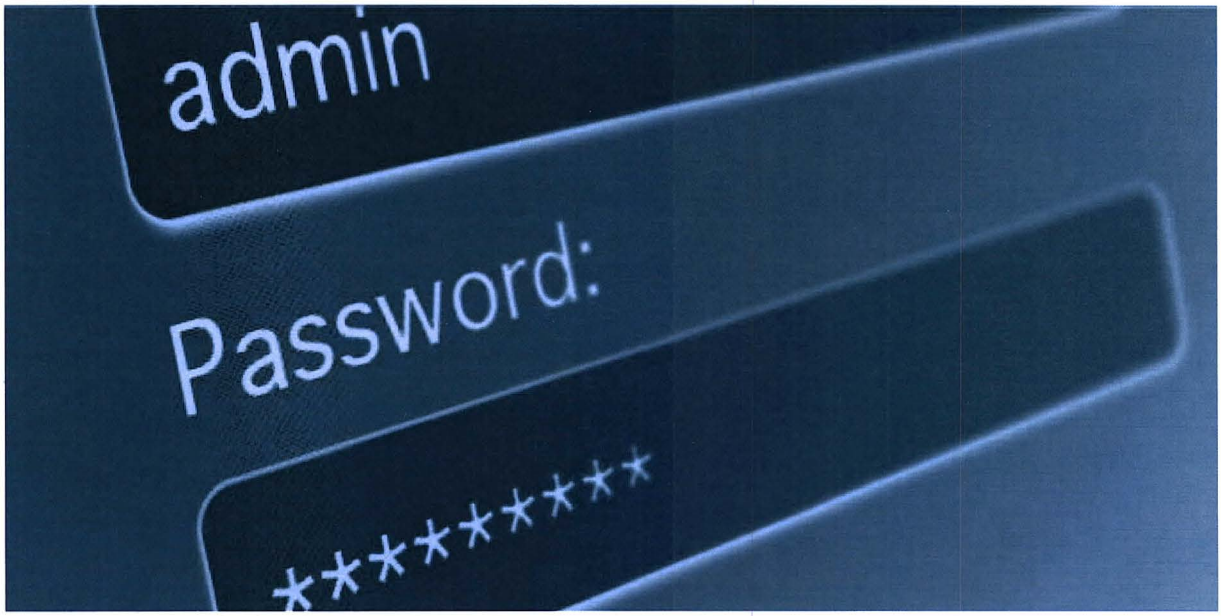
data brokers online privacy online shopping consumers privacy

JANUARY 26, 2017

Americans and Cybersecurity

Many Americans do not trust modern institutions to protect their personal data – even as they frequently neglect cybersecurity best practices in their own personal lives

BY KENNETH OLMSTEAD (HTTP://WWW.PEWINTERNET.ORG/AUTHOR/KOLMSTEAD/) AND AARON SMITH (HTTP://WWW.PEWRESEARCH.ORG/STAFF/AARON-SMITH/)



(jmiks/iStock.com)

Cyberattacks and data breaches are facts of life for government agencies, businesses and individuals alike in today's digitized and networked world. Just a few of the most high-profile breaches in 2016 alone include the hacking and subsequent release of emails (http://www.cbsnews.com/news/us-has-high-confidence-russian-intelligence-agency-hacked-dnc-dccc/) from members of the Democratic National Committee; the release of testing records of dozens of athletes (https://www.theguardian.com/sport/2016/nov/25/fancy-bears-hack-again-with-attack-on-senior-anti-doping-officials) conducted by the World Anti-Doping Agency; and the announcement by Yahoo (http://venturebeat.com/2016/12/14/yahoo-reveals-another-hack-where-unauthorized-third-party-stole-data-from-1-billion-accounts/) that hackers had accessed the private information associated with roughly 1 billion email accounts. Finally, in late 2016 and early 2017 U.S. intelligence agencies (the FBI, CIA and Department of Homeland Security) both issued

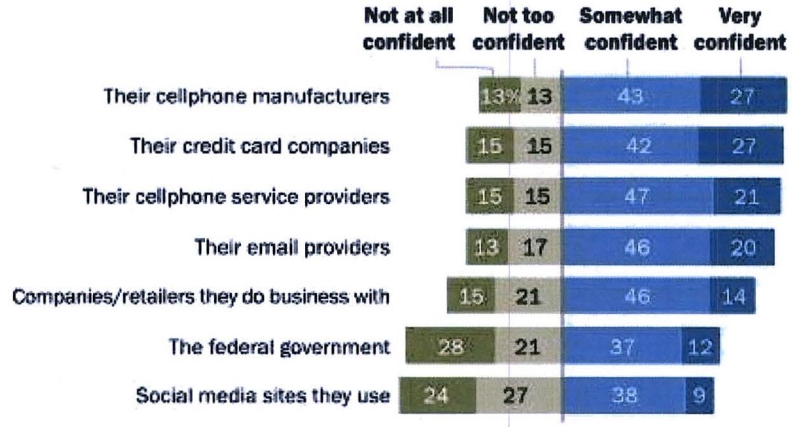
statements and testified before Congress (http://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-to-the-united-states) that the Russian government was involved in the hack of the DNC with the aim of influencing the 2016 presidential election.

Previous Pew Research Center studies of the digital privacy environment have found that many Americans fear they have lost control (http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/) of their personal information and many worry (http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/) whether government agencies and major corporations can protect the customer data they collect. As part of this ongoing series of studies (http://www.pewinternet.org/topics/privacy-and-safety/) on the state of online privacy and security, the Center conducted a national survey of 1,040 adults in the spring of 2016 to examine their cybersecurity habits and attitudes. This survey finds that a majority of Americans have directly experienced some form of data theft or fraud, that a sizeable share of the public thinks that their personal data have become less secure in recent years, and that many lack confidence in various institutions to keep their personal data safe from misuse. In addition, many Americans are failing to follow digital security best practices in their own personal lives, and a substantial majority expects that major cyberattacks will be a fact of life in the future. Among the key findings:

A majority of Americans (64%) have personally experienced a major data breach, and relatively large shares of the public lack trust in key institutions – especially the federal government and social media sites – to protect their personal information

Roughly half of Americans do not trust the federal government or social media sites to protect their data

% of U.S. adults/tech users (see note below) who are ___ in the ability of the following institutions to protect their data



Note: Data on cellphone manufacturers and service providers based on cellphone owners; data on email providers based on internet users; data on social media sites based on social media users. Data for credit card companies recalculated to exclude "does not apply" responses. Otherwise, refusals and "does not apply" responses not included in this chart.
Source: Survey conducted March 30-May 3, 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

(http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/pi_01-26-cyber-00-02/) Data security is a personal issue for many Americans: The survey finds that a majority of the public has noticed or been notified of a major data breach impacting their sensitive accounts or personal data. The survey examined several different types of data theft and found that 64% of U.S. adults have been impacted by at least one of them:

- 41% of Americans have encountered fraudulent charges on their credit cards.
- 35% have received notices that some type of sensitive information (like an account number) had been compromised.
- 16% say that someone has taken over their email accounts, and 13% say someone has taken over one of their social media accounts.
- 15% have received notices that their Social Security number had been compromised.
- 14% say that someone has attempted to take out loans or lines of credit in their name.
- 6% say that someone has impersonated them in order to file fraudulent tax returns.

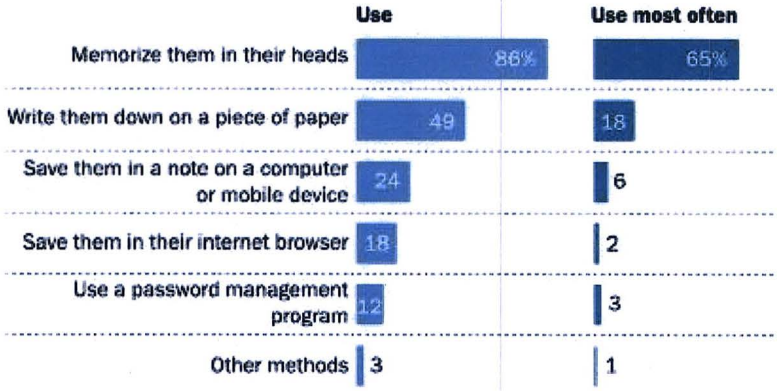
And beyond these specific experiences, roughly half of Americans (49%) feel that their personal information is less secure than it was five years ago. Around one-in-five (18%) feel that their information has gotten more secure in recent years, while 31% feel that their information is about as safe as it was five years ago. Americans age 50 and older are especially likely to feel that their personal information has become less safe in recent years: 58% of Americans in this age group express this opinion, compared with 41% of those ages 18 to 49.

In addition, many Americans lack faith in various public and private institutions to protect their personal information from bad actors. They express some level of concern about a variety of entities, ranging from telecommunications firms to credit card companies. But their fears are especially pronounced for two institutions in particular: the federal government and social media platforms. Some 28% of Americans are *not confident at all* that the federal government can keep their personal information safe and secure from unauthorized users, while 24% of social media users lack any confidence in these sites to protect their data. By contrast, just 12% of Americans (and 9% of social media users) have a very high level of confidence that these entities can keep their personal information safe and secure.

Many Americans fail to follow cybersecurity best practices in their own digital lives

Most Americans keep track of their online passwords by either memorizing them or writing them down

% internet users who keep track of their online passwords in the following ways



Note: Results for "use most often" category include those who use only one technique to manage their passwords.
Source: Survey conducted March 30-May 3 2016.
"Americans and Cybersecurity"

PEW RESEARCH CENTER

(http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/pi_01-26-cyber-00-01/) At the same time that they express skepticism about whether the businesses and institutions they interact with can adequately protect their personal information, a substantial share of the public admits that they do not always incorporate cybersecurity best practices into their own digital lives.

This lack of adherence to best practices begins with the ways that Americans keep track of the passwords to their online accounts. Cybersecurity experts generally recommend password management software as the safest and most secure way to track and maintain online passwords.

Still, just 12% of internet users say that they ever use password management software themselves – and only 3% say that this is the password technique they rely on most. Instead, roughly two-thirds (65%) of internet users say that memorization is the main or only way they keep track of their online passwords – and another 18% rely primarily on writing their passwords down on a piece of paper. In other words, fully 84% of online adults rely primarily on memorization or pen and paper as their main (or only) approach to password management.

Cybersecurity resources

Cybersecurity experts recommend a number of "best practices" and resources for consumers to minimize their exposure to security breaches.

General information on cybersecurity:

National Cyber Security Alliance StaySafeOnline.org (https://staysafeonline.org/)

Consumer information on online security from the Federal Trade Commission (https://www.consumer.ftc.gov/topics/online-security)

Top-10 safe computing tips from Information Systems and Technology at MIT (https://ist.mit.edu/security/tips)

Password management:

7 password experts on how to lock down your online security (https://www.wired.com/2016/05/password-tips-experts/)

PC Magazine: The best password managers of 2017 (http://www.pcmag.com/article2/0,2817,2407168,00.asp)

Using public Wi-Fi:

How to stay safe on public Wi-Fi (http://fieldguide.gizmodo.com/how-to-stay-safe-on-public-wifi-1779464400)

If your account has been hacked:

FBI Internet Crime Complaint Center (https://www.ic3.gov/default.aspx)

A substantial share of Americans are taking steps or following password protection strategies that experts recommend against:

- 41% of online adults have shared the password to one of their online accounts with a friend or family member.
- 39% say that they use the same (or very similar) passwords for many of their online accounts.
- 25% admit that they often use passwords that are less secure than they'd like, because simpler passwords are easier to remember than more complex ones.

The survey also finds that Americans are not always vigilant in the context of mobile security. For instance, 28% of smartphone owners report that they do not use a screen lock or other security features in order to access their phone, while around one-in-ten report that they never install updates to their smartphone's apps or operating system. Meanwhile, 54% of online adults report that they utilize potentially insecure public Wi-Fi networks – with around one-in-five of these users reporting that they use these networks to perform sensitive activities such as e-commerce or online banking.

To be sure, the story of cybersecurity is far from universally negative. For instance, roughly half of online adults (52%) report that they use two-step authentication on at least some of their online accounts. And majorities indicate that they do in fact take recommended steps such as utilizing different passwords from site to site or placing a security feature on their smartphones. But overall, the way that users treat and manage their online passwords and their overall digital security can be described as mixed at best.

Cybersecurity is not a top-of-mind worry for most Americans

Despite their concerns and experiences, most Americans do not express profound worries about cybersecurity in their personal lives or in their expectations for various public institutions.

In the context of their personal lives, fully 69% of online adults say they do not worry about how secure their online passwords are – more than double the share (30%) that admits to having worries about their personal password security. And Americans who have personally experienced a major data breach are generally no more likely than average to take additional means to secure their passwords (such as using password management software).

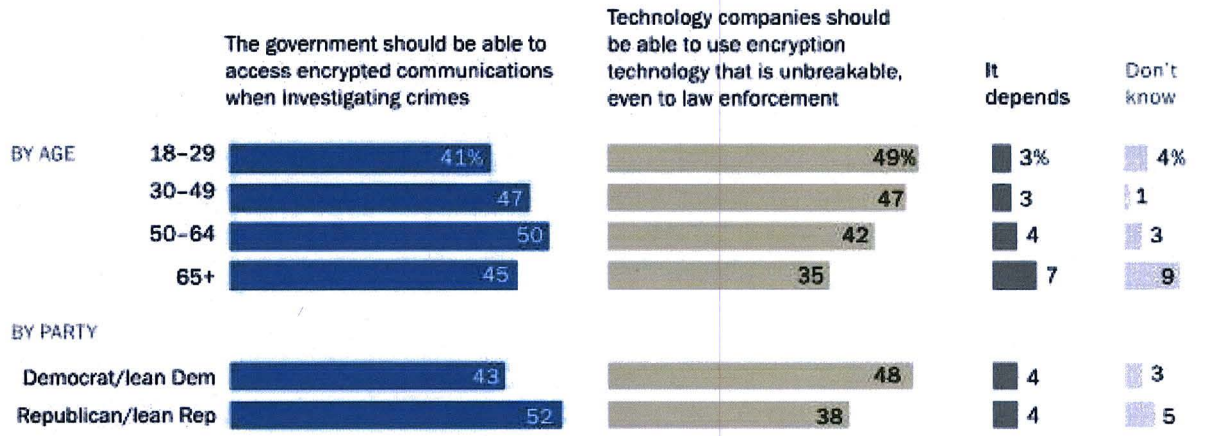
More broadly, a substantial majority of Americans anticipate major cyberattacks in the next five years on our nation's public infrastructure (70% expect that this will happen) or banking and financial systems (66%). Yet a majority of Americans feel that the U.S. government is at least somewhat prepared to handle cyberattacks on our public infrastructure (62%) or government agencies (69%), while 61% have some confidence that U.S. businesses are prepared to handle attacks on their own systems. However, it is worth noting that this survey was fielded prior to the revelations of some more recent, high-profile data breaches, including the hacking of the DNC email system and the breach of email accounts of Yahoo customers.

Americans continue to be highly divided on the issue of encryption

Americans remain divided on the issue of encryption: 46% believe that the government should be able to access encrypted communications when investigating crimes, while 44% believe that technology companies should be able to use encryption tools that are unbreakable even to law enforcement. Democrats and younger adults tend to express greater support for strong encryption, while Republicans tend to express greater support for encryption protocols that can be accessed by law enforcement in the context of criminal investigations.

Younger Americans express elevated support for unbreakable encryption standards

% of U.S. adults who agree with each statement



Source: Survey conducted March 30-May 3 2016
"Americans and Cybersecurity"

PEW RESEARCH CENTER

ABA BUSINESS LAW SECTION

KNOWLEDGE | COMMUNITY | EXPERIENCE

Volume 14, Number 2 - November/December 2004

Hey, that's personal!

When companies sell customer information gathered through the Internet

By Bethany Rubin Henderson

Imagine this: A new customer walks into your client's place of business. Within minutes your client knows *all* about that customer.

So what exactly is "all"? That would be his tastes and interests, how he prefers to shop (such as whether he browses the store at length or goes straight to the desired product), his purchasing habits, how he prefers to interact with your client's company (such as whether he reads posted signs and how he prefers to communicate with sales associates), what he is willing to pay for your client's products or services, and his contact information. Your client finds out all of this before the customer says a single word, and without the customer knowing that your client is gathering this information. Instantly — and without the customer even realizing it — your client's store morphs into an environment personalized entirely for that customer.

The result: an enormous boon to your client's bottom line. Sound unrealistic? In the bricks and mortar world, absolutely. However, thanks to Internet technology, any company with a Web site can do this. Many already are.

Sure, you may say, that sounds wonderful, but how can that be lawful? With all of the press about identity theft these days, and federal legislation such as the 2003 USA Patriot Act and Homeland Security Act, there must be laws prohibiting my client from surreptitiously gathering and using such information. Surprisingly, very few such laws are on the books.

However, a legal regime is slowly developing, and the Federal Trade Commission

and certain states recently have begun taking a very active role in ensuring compliance with fair information practices. This article reviews what every in-house counsel and business lawyer should know about commercial clients' collection, use and sale of the personally identifiable information of online customers.

Web sites that do not cull their visitors' information may be at a distinct disadvantage in the marketplace. The vast majority of companies with Web sites *do* collect personally identifiable information from online visitors, and, according to a recent FTC study, more than two-thirds collect nonpersonally identifiable information as well. Some of the more common methods used to collect such information are:

- *Requesting it voluntarily* — Most Web sites require that visitors who purchase goods or services take part in online contests or surveys, or who register to use a Web site or an online service voluntarily provide contact and billing information. It is becoming increasingly common in some industries to require a visitor to provide contact information, or at least to register a username and password, before allowing her to even browse a Web site.

  Many sites request far more information than is required for any particular transaction, and all but the savviest Internet users usually willingly provide it. It is increasingly common for Web sites to offer visitors the choice to opt out of certain uses of their personal data, but many visitors do not bother to change a default setting of opting in;
- *Spyware* — There are various types of software that may be placed on a Web site visitor's computer, without his knowledge, to transmit information about the Internet habits and interests of that computer's users back to the company that installed the device. Two of the most common and well-known tracking devices are Web bugs (graphic image files embedded in a Web page that are invisible to the naked eye) and cookies (files sitting on a computer's hard drive); and
- *Tracking clickstreams* — Certain types of software and spyware programs enable companies to track the pattern and order of visitors' mouse movements and clicks within and across Web sites.

It is common to use multiple data-gathering tools simultaneously. These technologies, especially when used in conjunction with each other, make it possible to track a Net user's online behavior over an extended period of time, often regardless of whether she knows of or consents to the collection of that information, and even if she logs on and off the Internet or periodically shuts down and re-starts her computer.

More important, they allow the easy correlation of individual Web site visitors' personally identifiable information with nonpersonally identifiable information. These compilations can be used to create profiles of individual Internet users, which can be highly valuable. For example, such profiles may be used, among other things:

- to predict a Web site visitor's interests and purchasing habits, thereby making it possible to target ads, prices and content directly to that individual;
- for internal market research and development;
- for direct profit by selling customer lists, information and preferences to third parties; and
- to market other products or services.

Industry and third-party privacy organizations have rushed to fill the void left by the dearth of federal legislation concerning online consumer privacy. For many years, the FTC supported industry self-regulation and took little direct action itself against companies that abused customer data they collected online. As a result, several industry organizations created their own standards for their members' online collection and use of consumers' personally identifiable information.

Additionally, numerous third-party seal programs purport to independently monitor Web sites' information collection and use practices. Seal programs typically offer a branded privacy seal and public recognition to those Web sites that abide by their recommended privacy practices. *(See sidebar on*

third-party privacy guidelines.)

Self regulation and third-party regulation has proven to be relatively ineffective because the rules governing the use of personally identifiable information are not uniform. Although virtually all of the third-party privacy guidelines center on the commonly accepted fair information practice principles of notice, choice, access and security, each program has developed its own distinct — and often-competing — set of rules particular to its own membership and goals.

Many companies also create their own unique privacy practices, which may be inconsistent with those recommended by industry or third-party privacy organizations. Consequently, the online collection and use of personally identifiable information is inconsistent even within industries.

Furthermore, enforcement of these self-imposed guidelines is greatly limited. Most industry-promulgated and third-party guidelines have minimal enforcement mechanisms. Commercial entities are not required to join privacy seal programs, and compliance with internal privacy policies depends largely on self-reporting. In short, without the threat of legal sanctions, companies have little to no incentive to audit their adherence to any privacy practices.

The FTC recognized these shortcomings and recently has reversed its long-held position that online consumer privacy protection should be left to industry self- regulation. The FTC has begun to hold forums on topics such as spyware and to issue public opinion letters about various online consumer privacy issues and practices. Over the last five years, the FTC also has started pursuing litigation and administrative actions against companies that egregiously abuse customers' privacy or deceptively collect or use online consumers' personally identifiable information.

The FTC has prosecuted several different companies (most recently Tower Records) for permitting security flaws in their Web sites and computer systems that made consumers' personally identifiable information vulnerable to exposure to third parties in violation of those companies' privacy policies. The FTC also has pursued actions against numerous companies for deceptively collecting, using and selling personally identifiable information from online consumers, as well as for making false statements about online information collection practices and security.

For example, the FTC recently prosecuted Gateway Learning, best known for its "Hooked on Phonics" products, for engaging in unfair and deceptive trade practices related to its renting of online customers' personally identifiable information to third-party marketers. See *In the Matter of Gateway Learning Corp.*,FTC File No. 042-3047. GeoCities, ToySmart.com, Microsoft and Guess.com also have been recent targets of the FTC's crackdown on corporate abuse or misuse of online consumers' personally identifiable information.

The case of Gateway Learning is particularly instructive. Gateway Learning collected personally identifiable information from online consumers under a privacy policy that expressly promised that collected information would not be sold, and that consumers would be given the opportunity to opt out of any future sale if the policy changed.

Nevertheless, in 2003, Gateway Learning began to rent out customers' information to third-party marketers, and changed its privacy policy retroactively to permit such activities, without notifying its consumers or obtaining their consent. The FTC charged Gateway Learning with violating Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices.

In July 2004, the parties reached a settlement agreement that, among other things, bars Gateway Learning from sharing any online customer's personal information without affirmative opt-in consent, prohibits Gateway Learning from retroactively changing its privacy policy without customer consent, and

requires Gateway Learning to relinquish all profits from the rental of its online customers' information.

Neither federal nor state legislation has caught up with the FTC. Today there still is no unified regulatory scheme governing what sort of personally identifiable information lawfully can be collected online (or offline) by commercial entities or how such information can be used or disseminated after it is collected. The federal legislation that does regulate what commercial entities may do with consumer information is piecemeal and typically focuses on a particular type of personally identifiable information or a particular use of that information. For example, multiple statutes regulate identity theft, and several new bills on that subject were introduced in the 108th Congress (such as S.153, S.223, H.R.1731 & H.R.2035).

Industry-specific legislation restricting the use and dissemination of certain types of personal information also abounds. *(See the sidebar on industry-specific federal legislation.)* Although Congress has so far taken only a piecemeal approach to protecting consumer privacy, these disparate statutes and bills, taken together, show Congress' willingness both to protect individual privacy and to punish those who fail to respect the awesome responsibility that comes with the possession of personally identifiable information.

Recently, Congress has begun to recognize that Internet technology poses new challenges to personal privacy that cannot be sufficiently circumscribed by the existing piecemeal legislation. To date, only two federal laws directly address the Internet environment and regulate the collection and use of personally identifiable information gathered from Web site visitors. Although debate rages about the efficacy and enforceability of both statutes, they demonstrate Congress' willingness to legislate in the online arena.

One of those statutes is the Children's Online Privacy Protection Act, 15 U.S.C. §6501 (1998) (COPPA). COPPA restricts both Web sites targeted at children younger than 13, and those who knowingly collect information online from such children, from collecting and using children's personally identifiable information without verifiable parental consent.

The other statute is the Controlling the Assault of Non- Solicited Pornography and Marketing Act, 15 U.S.C. 7701 (2003) (CAN-SPAM Act). CAN-SPAM focuses primarily on regulating the identification and transmission of unsolicited marketing and sexually explicit e-mails. However, it also contains restrictions on the gathering and use of personal e-mail addresses. CAN-SPAM requires that conspicuous notice be given to e-mail recipients on how to opt out of receiving e-mails, and prohibits e- mailing those who do opt out.

It forbids knowingly sending commercial e-mails to addresses collected by Web sites with privacy notices stating that the Web-site operator will not disseminate e-mail addresses it collects. CAN-SPAM also proscribes knowingly sending commercial e-mails to addresses identified through automated harvesting (that is, combining names, letters or numbers in various permutations through automated means). Violations of both COPPA and the CAN-SPAM Act are explicitly deemed unfair and deceptive trade practices under the Federal Trade Commission Act.

To date, no single federal law regulates what companies can do with the other personally identifiable information they gather from *adult* Internet users. However, the absence of such legislation should not be seen as suggesting that Congress is not interested in this particular subject. In fact, in each of the last several sessions of Congress, multiple bills specifically targeted at restricting the collection, use and sale of information gathered online were introduced in both houses.

During the 107th Congress, several bills in both houses aimed to regulate the online collection and use of personally identifiable information. The broadest ones were the Senate's Online Privacy Protection Act (S.2201) and the House of Representatives' Consumer Privacy Protection Act of 2002 (H.R. 4678). The

Senate bill explicitly recognized the unique dangers to privacy posed by the Internet, while the House bill addressed consumer privacy generally. Both bills provided for enforcement by the FTC. The Senate bill also authorized limited private and state actions for certain violations. However, neither bill made it very far. The Senate bill was placed on the Senate calendar, but no action was ever taken on it. The House bill never even made it out of committee.

Many more bills addressing the use and dissemination of personally identifiable information have been introduced in the 108th Congress to date. Restricting commercial installation and use of spyware — which is viewed as particularly insidious by many legislators and privacy advocates — has been a favorite subject of recent legislative proposals. In fact, in October the House passed two separate anti-spyware bills, which are now awaiting review by the Senate. (H.R.4661 and H.R. 2929). Restrictions on the collection and commercial use of distinct types of personally identifiable data, including Social Security numbers and TV viewing preferences, also has remained popular in the 108th Congress.

While most of the legislative proposals in Congress target specific types or uses of personal data, four bills broadly aim to restrict the collection and use of online or electronic data. Those bills are:

- Privacy Act of 2003 (S.745): seeks to prohibit commercial entities from disclosing or selling to third parties any personally identifiable customer information collected either online or offline without first notifying those individuals whose information has been collected and providing them adequate opportunity to restrict or opt out of the sale of their information;
- Online Privacy Protection Act of 2003 (H.R.69): proposes restrictions on the online use and collection of personally identifiable information of persons not covered by COPPA;
- Notification of Risk to Personal Data Act (S.1350): seeks to require those engaged in interstate commerce to disclose the unauthorized acquisition of electronic data containing personal information; and
- Consumer Privacy Protection Act of 2003 (H.R.1636): a comprehensive bill with language broadly aimed at protecting personally identifiable information in a variety of contexts.

Despite the abundance of recent legislative proposals about online consumer privacy, none of the proposed bills has advanced to a full floor vote. In fact, most have languished in committee. However, the various proposals share many similarities with each other, with COPPA, and with those portions of the CAN-SPAM Act regulating the collection, sale and use of personal e- mail addresses. Taken together they provide a roadmap to what sort of regulations Congress may impose on the online collection and use of adults' personally identifiable information.

First, they generally direct that adequate and accurate notice be given to those persons whose information is being collected about how that information will be collected, used and disseminated. Second, they generally require that the individual whose data is at issue consents to its collection and use. Most commonly, the proposed bills approve the use of opt-out mechanisms to accomplish this feat. Finally, and most important, these bills provide for meaningful enforcement mechanisms.

Virtually all of the proposed legislation explicitly lodges enforcement authority in the FTC. Most of the bills explicitly classify violations of their provisions as violations of the unfair and deceptive trade practices provisions of the Federal Trade Commission Act. One, the Privacy Act of 2003 (S.745), also contains a safe harbor provision excluding from its mandate those commercial entities that comply with FTC-approved self- regulatory guidelines issued by industry or third-party privacy seal organizations. Some proposed bills also expressly grant states or private individuals limited rights to pursue civil actions for certain violations.

The volume of legislation proposed in the 107th and 108th Congresses that was directed at commercial entities' online collection, use and dissemination of personally identifiable information suggests that federal legislation on these topics may well be coming. The similarities in those bills reveal that the FTC

is likely to be the primary enforcement authority and that the Federal Trade Commission Act's prohibition against unfair and deceptive trade practices likely will set the standard by which companies' actions will be measured.

Further, the FTC's stepped-up activities — despite the absence of federal legislation — coupled with recent actions by states such as New York, Texas and Michigan against private companies that violate their own online data collection privacy policies or abuse the privacy of online consumers, demonstrate that commercial entities engaging in the online collection, use and dissemination of personally identifiable information should be circumspect.

This does not mean that companies should stop collecting and using such data. In fact, personally identifiable data is so valuable that any commercial entity that does not take advantage of every opportunity to collect and use such information is likely to quickly find itself at a competitive disadvantage. However, at a minimum, companies can and should adhere to standard fair information practice guidelines to protect themselves from future litigation or hefty penalties.

Third-party privacy guidelines

Industry organizations with online consumer privacy guidelines include:

- *Online Privacy Alliance*: a cross-industry coalition of nearly 100 global companies. (http://www.privacyalliance.org)
- *Network Advertising Initiative*: an organization of companies that facilitate Web advertising through ad serving, hosting and ad sales services. (http://www.networkadvertising.org)
- *Direct Marketing Association*: the trade organization for direct marketers. (http://www.the-dma.org/privacy/index.shtml)

Some of the more widely recognized third-party seal programs are:

- The Better Business Bureau Online (https://www.bbbonline.org/privacy)
- TRUSTe(http://www.truste.org)
- PrivacyBot (http://www.privacybot.com)

Industry-specific federal legislation

Federal legislation targeting consumer privacy crosses virtually every industry. Some of the more prominent federal statutes restricting what companies can do with customers' personally identifiable data are:

- Electronic Communications Privacy Act of 1986, 18 U.S.C. §2701: prohibits electronic communication service providers from disclosing the contents of the electronic communications stored on their servers.
- Cable Communications Policy Act, 47 U.S.C. §551: regulates cable television companies' collection and use of customers' personal data.
- Video Privacy Protection Act, 18 U.S.C. §2710: restricts disclosure of customers' personal information and video rental practices and preferences by videotape sale or rental companies.
- Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq.*: regulates the collection and use of consumer credit information.
- Gramm-Leach-Bliley Act, 15 U.S.C. §6801 *et seq.*: regulates the disclosure of nonpublic personal information by financial institutions.
- Health Insurance Portability and Accountability Act of 1996: regulates the collection, use and dissemination of patients' medical records and information.

Best practices

Have a transparent and conspicuous privacy policy that is readily accessible to Web site visitors, and strictly adhere to it;

- Notify customers whose information has been collected in advance of any material changes to your privacy policy and give them the opportunity either to opt out of the changes or to delete their personally identifiable information from your database;
- Join an independent seal program and adhere to its privacy practices;
- Provide a meaningful mechanism for visitors to opt out of having their information either collected while browsing your Web site or used in particular ways, and scrupulously honor all opt-out requests;
- Maintain personal data collected online in a secure environment in accordance with a clear privacy policy, and repeatedly review and update security mechanisms to ensure that no vulnerabilities exist; and
- Do not sell a Web site visitor's personally identifiable information to third parties without either the visitor's express prior permission or without making an explicit and conspicuous public announcement of your intentions and providing a meaningful opt-out mechanism.

— Bethany Rubin Henderson

Henderson is an associate at Quinn Emanuel Urquhart Oliver & Hedges, LLP, in Los Angeles. Her e-mail is bethanyhenderson@quinnemanuel.com.

Back to Top

Right to Know Act (AB 1291)

Author : Assembly Member Bonnie Lowenthal

The California Right to Know Act (AB 1291- Lowenthal) will modernize current privacy law and give Californians an effective tool to monitor how personal information, including about health, finances, your location, politics, religious, sexual orientation, buying habits, and more, is being collected and disclosed in unexpected and potentially harmful ways.

Did you know?

- Websites incorporate up to 100 tracking tools that collect personal information about visitors like age, gender, race, income, health concerns and recent purchases for advertising and marketing companies.
- Many mobile apps share location, age, gender, phone numbers, and other personal details of both adults and children with third party companies. Women and children have been hurt or killed when location data was shared with abusers.
- Facebook apps used by a consumer's "friend" can often access sensitive information about that consumer, including religious, political, and sexual preferences. (use link currently on AB 1291 page and link to our FB app when it is up again)
- Companies that collect information about consumer activities have exposed sensitive personal information. Target revealed that a woman was pregnant and Facebook outed the sexual orientation of a college student before they told their families.
- Data brokers are engaged in the widespread buying, selling, and trading of personal information obtained from mobile phones, banks, social media sites, and stores. Americans have lost jobs and been denied mortgages when data brokers shared incorrect information and scammers use data broker lists to target vulnerable populations like seniors.

The White House, Federal Trade Commission, and California Attorney General all call for data transparency and access for consumers. AB 1291 would meet that call by giving Californians the Right to Know.

What's happening to your personal information? It's time to demand the Right to Know so you can better protect your privacy, personal safety, and financial security. Contact your legislator today and urge them to support the Right to Know Act.

The California Right to Know Act is authored by Assemblymember Bonnie Lowenthal (D-Long Beach), co-sponsored by the ACLU of California and supported by a diverse coalition of organizations that work every day to safeguard the privacy, personal safety, and financial security of Californians and their families.

UPDATES

01/31/2014
Failed to pass through the Assembly Judiciary Committee.

05/23/2013
AB 1291 is now a two-year bill.

02/23/2013
AB 1291 is introduced to give Californians the right to know how their personal information is shared and collected online.

Issues : Privacy and Government Surveillance, Technology and Civil Liberties

Content, Context, and Control: Facial Recognition and Privacy

ACLU-NC Invited to White House Summit on Cybersecurity & Consumer Protection

License Plate Readers in Alameda Need Strict Privacy Safeguards

DOI:10.1145/1743546.1743558

Arvind Narayanan and Vitaly Shmatikov

Privacy and Security
Myths and Fallacies of "Personally Identifiable Information"

Developing effective privacy protection technologies is a critical challenge for security and privacy research as the amount and variety of data collected about individuals increase exponentially.

THE DIGITAL ECONOMY relies on the collection of personal data on an ever-increasing scale. Information about our searches, browsing history, social relationships, medical history, and so forth is collected and shared with advertisers, researchers, and government agencies. This raises a number of interesting privacy issues. In today's data protection practices, both in the U.S. and internationally, "personally identifiable information" (PII)—or, as the U.S. Health Insurance Portability and Accountability Act (HIPAA) refers to it, "individually identifiable" information—has become the *lapis philosophorum* of privacy. Just as medieval alchemists were convinced a (mythical) philosopher's stone can transmute lead into gold, today's privacy practitioners believe that records containing sensitive individual data can be "de-identified" by removing or modifying PII.

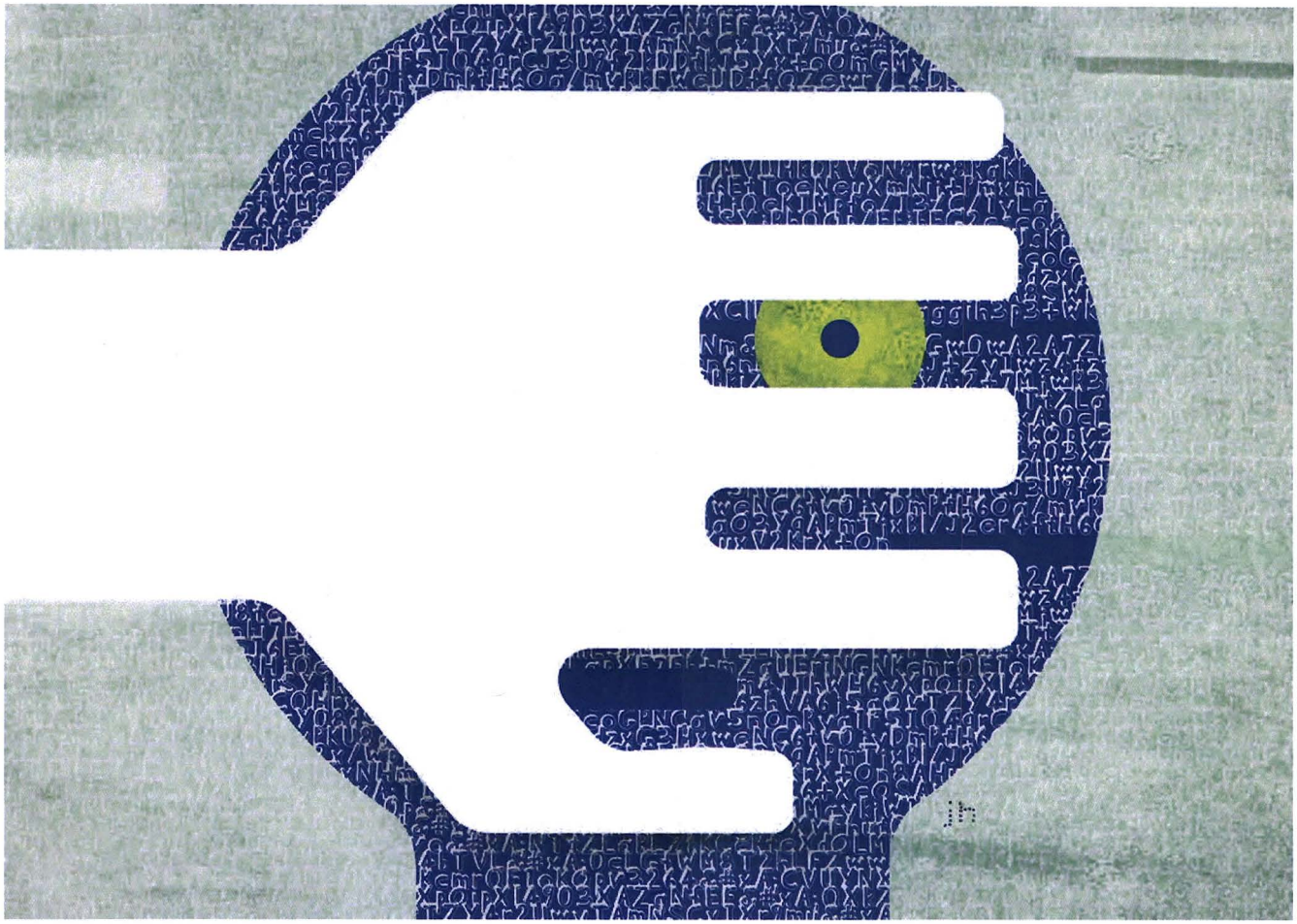
Any information that distinguishes one person from another can be used for re-identifying data.

What is PII?

For a concept that is so pervasive in both legal and technological discourse on data privacy, PII is surprisingly difficult to define. One legal context is provided by breach-notification laws. California Senate Bill 1386 is a representative example: its definition of personal information includes Social Security numbers, driver's license numbers, financial accounts, but not, for example, email addresses or telephone numbers. These laws were enacted in response to security breaches involving customer data that could enable identity theft. Therefore, they focus solely on the types of data that are commonly used for authenticating an individual, as opposed to those that violate privacy, that is, reveal some sensitive information about an individual. This crucial distinction is often overlooked by designers of privacy protection technologies.

The second legal context in which the term "personally identifiable information" appears is privacy law. In the U.S., the Privacy Act of 1974 regulates the collection of personal information by government agencies. There is no overarching federal law regulating private entities, but some states have their own laws, such as California's Online Privacy Protection Act of 2003. Generic privacy laws in other countries include Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and Directive 95/46/EC of the European Parliament, commonly known at the Data Protection Directive.

Privacy laws define PII in a much broader way. They account for the possibility of deductive disclosure and—unlike breach-notification laws—do not lay down a list of informational



attributes that constitute PII. For example, the Data Protection Directive defines personal data as: "any information relating to an [...] natural person [...] who can be identified, directly or indirectly, in particular by reference [...] to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity."

The Directive goes on to say that "account should be taken of all the means likely reasonably to be used either by the controller[a] or by any other person to identify the said person." Similarly, the HIPAA Privacy Rule defines individually identifiable health information as information "1) That identifies the individual; or 2) With respect to which there is a reasonable basis to believe the information can be used to identify the individual." What is "reasonable"? This is left open to interpretation by case law. We are not aware of any court decisions that define identifiability in the context of HIPAA.[b] The "safe harbor" provision of the Privacy Rule enumerates 18 specific identifiers that must be removed prior to data release, but the list is not intended to be comprehensive.

PII and Privacy Protection Technologies

Many companies that collect personal information, including social networks, retailers, and service providers, assure customers that their information will be released only in a "non-personally identifiable" form. The underlying assumption is that "personally identifiable information" is a fixed set of attributes such as names and contact information. Once data records have been "de-identified," they magically become safe to release, with no way of linking them back to individuals.

The natural approach to privacy protection is to consider both the data and its proposed use(s) and to ask: What risk does an individual face if her data is used in a particular way? Unfortunately, existing privacy technologies such as *k*-anonymity[6] focus instead on the data alone. Motivated by an attack in which hospital discharge records were re-identified by joining[c] them via common demographic attributes with a public voter database,[5] these methods aim to make joins with external datasets harder by anonymizing the identifying attributes. They fundamentally rely on the fallacious distinction between "identifying" and "non-identifying" attributes. This distinction might have made sense in the context of the original attack, but is increasingly meaningless as the amount and variety of publicly available information about individuals grows exponentially.

To apply *k*-anonymity or its variants such as *l*-diversity, the set of the so-called *quasi-identifier* attributes must be fixed in advance and assumed to

a The individual or organization responsible for the safekeeping of personal information.

b When the Supreme Court of Iceland struck down an act authorizing a centralized database of "non-personally identifiable" health data, its ruling included factors such as education, profession, and specification of a particular medical condition as part of "identifiability."

c In the sense of SQL join.

ILLUSTRATION BY JOHN HERSEY

be the same for all users. It typically includes ZIP code, birth date, gender, and/or other demographics. The rest of the attributes are assumed to be non-identifying. De-identification involves modifying the quasi-identifiers to satisfy various syntactic properties, such as "every combination of quasi-identifier values occurring in the dataset must occur at least k times."[6] The trouble is that even though joining two datasets on common attributes can lead to re-identification, anonymizing a predefined subset of attributes is not sufficient to prevent it.

Re-identification without PII

Any information that distinguishes one person from another can be used for re-identifying anonymous data. Examples include the AOL fiasco, in which the content of search queries was used to re-identify a user; our own work, which demonstrated feasibility of large-scale re-identification using movie viewing histories (or, in general, any behavioral or transactional profile[2]) and local structure of social networks;[3] and re-identification based on location information and stylometry (for example, the latter was used to infer the authorship of the 12 disputed Federalist Papers).

Re-identification algorithms are agnostic to the semantics of the data elements. It turns out there is a wide spectrum of human characteristics that enable re-identification: consumption preferences, commercial transactions, Web browsing, search histories, and so forth. Their two key properties are that (1) they are reasonably stable across time and contexts, and (2) the corresponding data attributes are sufficiently numerous and fine-grained that no two people are similar, except with a small probability.

The versatility and power of re-identification algorithms imply that terms such as "personally identifiable" and "quasi-identifier" simply have no technical meaning. While some attributes may be uniquely identifying on their own, *any attribute can be identifying in combination with others*. Consider, for example, the books a person has read or even the clothes in her wardrobe: while no single element is a (quasi)-identifier, any sufficiently large subset uniquely identifies the individual.

Re-identification algorithms based on behavioral attributes must tolerate a certain "fuzziness" or imprecision in attribute values. They are thus more computationally expensive and more difficult to implement than re-identification based on demographic quasi-identifiers. This is not a significant deterrence factor, however, because re-identification is a one-time effort and its cost can be amortized over thousands or even millions of individuals. Further, as Paul Ohm argues, re-identification is "accretive": the more information about a person is revealed as a consequence of re-identification, the easier it is to identify that person in the future.[4]

Lessons for Privacy Practitioners

The emergence of powerful re-identification algorithms demonstrates not just a flaw in a specific anonymization technique(s), but the fundamental inadequacy of the entire privacy protection paradigm based on "de-identifying" the data. De-identification provides only a weak form of privacy. It may prevent "peeping" by insiders and keep honest people honest. Unfortunately, advances in the art and science of re-identification, increasing economic incentives for potential attackers, and ready availability of personal information about millions of people (for example, in online social networks) are rapidly rendering it obsolete.

The PII fallacy has important implications for health-care and biomedical datasets. The "safe harbor" provision of the HIPAA Privacy Rule enumerates 18 attributes whose removal and/or modification is sufficient for the data to be considered properly de-identified, with the implication that such data can be released without liability. This appears to contradict our argument that PII is meaningless. The "safe harbor" provision, however, applies only if the releasing entity has "no actual knowledge that the information remaining could be used, alone or in combination, to identify a subject of the information." As actual experience has shown, any remaining attributes can be used for re-identification, as long as they differ from individual to individual. Therefore, PII has no meaning even in the context of the HIPAA Privacy Rule.

Beyond De-identification

Developing effective privacy protection technologies is a critical challenge for security and privacy research. While much work remains to be done, some broad trends are becoming clear, as long as we avoid the temptation to find a silver bullet. Differential privacy is a major step in the right direction.[1] Instead of the unattainable goal of "de-identifying" the data, it formally defines what it means for a *computation* to be privacy-preserving. Crucially, it makes no assumptions about the external information available to the adversary. Differential privacy, however, does not offer a universal methodology for data release or collaborative, privacy-preserving computation. This limitation is inevitable: privacy protection has to be built and reasoned about on a case-by-case basis.

Another lesson is that an interactive, query-based approach is generally superior from the privacy perspective to the "release-and-forget" approach. This can be a hard pill to swallow, because the former requires designing a programming interface for queries, budgeting for server resources, performing regular audits, and so forth.

Finally, any system for privacy-preserving computation on sensitive data must be accompanied by strong access control mechanisms and non-technological protection methods such as informed consent and contracts specifying acceptable uses of data. C

References

1. Dwork, C. A firm foundation for private data analysis. *Commun. ACM.* (to appear).
2. Narayanan, A. and Shmatikov, V. Robust de-anonymization of large sparse datasets. In *Proceedings of the 2008 IEEE Symposium on Security and Privacy.*
3. Narayanan, A. and Shmatikov, V. De-anonymizing social networks. In *Proceedings of the 2009 IEEE Symposium on Security and Privacy.*
4. Ohm, P. Broken promises of privacy: Responding to the surprising failure of anonymization. 57 *UCLA Law Review 57*, 2010 (to appear).
5. Sweeney, L. Weaving technology and policy together to maintain confidentiality. *J. of Law, Medicine, and Ethics 25* (1997).
6. Sweeney, L. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal on Uncertainty, Fuzziness, and Knowledge-Based Systems 10* (2002).

Arvind Narayanan (arvindn@cs.utexas.edu) is a postdoctoral fellow at Stanford University. **Vitaly Shmatikov** (shmat@cs.utexas.edu) is an associate professor of computer science at the University of Texas at Austin. Their paper on de-anonymization of large sparse datasets[2] received the 2008 PET Award for Outstanding Research in Privacy Enhancing Technologies.

2012

The Challenge of "Big Data" for Data Protection

Fred H. Cate
Indiana University Maurer School of Law, fcate@indiana.edu

Christopher Kuner
Brussels Privacy Hub

Christopher Millard
Cloud Legal Project

Dan Jerker B. Svantesson
Bond University

Editorial

The challenge of 'big data' for data protection

Christopher Kuner*, Fred H. Cate**, Christopher Millard**, and Dan Jerker B. Svantesson***

Data protection, like almost everything else in our lives, is challenged by the advent of 'big data'. The *Economist* reports in its 2012 Outlook that the quantity of global digital data expanded from 130 exabytes in 2005 to 1,227 in 2010, and is predicted to rise to 7,910 exabytes in 2015.[1]

An exabyte is a quintillion bytes. If you find that hard to visualize, consider this: someone has calculated that if you loaded an exabyte of data on to DVDs in slimline jewel cases, and then loaded them into Boeing 747 aircraft, it would take 13,513 planes to transport one exabyte of data. Using DVDs to move the data collected globally in 2010 would require a fleet of more than 16 million jumbo jets.

And exabytes are rapidly becoming passé. The volume of stored information in the world is growing so fast that scientists have had to create new terms, including zettabyte and yottabyte, to describe the flood of data.

The importance of big data is not just a result of its size or how fast it is growing (about 60 per cent a year), but also the reality that the data come from an amazing array of sources. The Internet captures lots of data. Facebook alone has more than 800 million active users, more than half of whom log in every day, where they generate more than 900 million web pages and upload more than 250 million photos every day.

In 2010, a lifetime ago in Internet time, Google sites were used by more than 1 billion unique visitors every month who spent a collective 200 billion minutes on its sites. Google-owned YouTube passed 1 trillion video playbacks in 2011. Email, IM, VOIP calls, and other communications generate tens of trillions of recorded messages every year.

Credit and debit cards, checks, and other financial activities provide a steady stream of billions of financial transactions recorded every month.

And increasingly sensor networks—video surveillance cameras, embedded computers in automobiles, the more than 5 billion cell phones we carry—record locations, movements, and activities. We can now talk meaningfully about ubiquitous data collection, in which almost everything we do results in data being captured and stored by one or more third parties.

It is significant that those data are digital. They can be stored, shared, searched, combined, and duplicated with extraordinary speed and at very little cost. And they are accompanied by metadata—data about when and where and how the underlying information was generated. Some experts estimate that there may be five times more metadata than the information we are aware of creating, and this metadata can be extraordinarily revealing.

We used to define 'big data' as being data sets so large that a supercomputer was needed to process them, but another aspect of big data has been that not only has analytical capacity soared, but also become far more inexpensive and widely distributed. It is not just that today's mobile devices have more computing power than the desktop machines of a decade ago, but also that we can now link data and computers virtually so that huge computational tasks can be undertaken affordably and conveniently.

In fact, we are witnessing the movement of more of that computational power, as well as storage of the tidal wave of data we are generating and collecting, into the 'cloud'. Cloud computing is all the rage, but despite the overuse and misuse of the term, it is increasingly clear that many of the data and resources we used to believe that we had to possess locally—in computers, handheld devices, entertainment systems, and business record systems—can now be provided with greater security and reliability (and at lower cost) remotely.

When thinking about the importance of 'big data', it is critical to remember that access to so much data, from so many different sources, and to the computing

* Editor-in-Chief
** Editor
***Managing Editor

1 'Welcome to the yotta world', The Outlook for 2012, *Economist*, Dec. 2011; http://www.economist.com/node/2 1537922.

power necessary to process it, increasingly means we can perceive patterns, engage in discoveries, and discover secrets that were heretofore hidden.

This new-found power has already yielded fabulous successes in fields such as medical research, where drug interactions and the efficacy of treatments can be assessed in ways never before possible and without endangering lives through interventional research. But the same capacity has been shown to make deidentification more difficult, as Google and Netflix discovered when making available anonymized data sets for research.

One significant result of, and contributor to, big data development is how much we rely on data-based systems for critical decisions and applications. It is no exaggeration to say that we are nothing more than a collection of data to most of the institutions—and many of the people—with whom we deal. It is not simply that 'our biographies are etched in the ones and zeros we leave behind in daily digital transactions,' as Stanford Law School Professor Kathleen Sullivan has written,[2] it is that it is those collections of zeros and ones are what identify, describe, and increasingly define us to others.

Big data poses enormous challenges for data protection—both by processors and regulators. It simultaneously changes the context and raises the stakes for data protection. Not surprisingly, given the pace of the change, there is little evidence that data protection is keeping up.

Consider, for example, the fascination shown by the EU data protection directive and the proposed EU General Data Protection Regulation, similarly to law in most of the rest of the world, with 'notice' and 'choice' or 'consent' as key tools of data protection. Despite mounting evidence that individuals ignore notices, often do not understand the choices (which often aren't meaningful in any event), and resist making them unless compelled to do so (in which case they almost always make the choice required to obtain the desired service or product), regulators continue to cling to these concepts. But irrespective of the success of notice and choice to date, how will these tools fare in a world of ubiquitous surveillance, and thousands of data exchanges by and about every individual on the planet every day? In short order the largest database on the planet may be of legally required privacy notices that no one has read.

Even where legislative drafters demonstrate awareness that data processing on a very large scale may raise particular concerns, evidence that the practical risk implications are understood may be lacking. For example, the draft EU General Data Protection Regulation provides for an exception to the general prohibition on transfers of personal data to countries that lack adequate protection where a transfer 'cannot be qualified as frequent and massive'.[3] While the use of the term 'massive' hints at an appreciation of the challenge of big data, no attempt is made to define the concept or even to put it in a relative context.

Big data will also place data protection in a different context. We often talk about data being the 'currency' of the information age, but in a world in which data represent individuals in more and more transactions, and provide the basis for decision making, issues such as the accessibility, accuracy, and reliability of data may matter as much or maybe more than privacy.

This seems especially likely to prove true with cloud computing. Just as national security has tended to trump privacy in most anti-terrorism and law enforcement programmes, as critical data and applications are stored remotely, accessibility may become more important than privacy.

Big data also ratchet up the importance of harmonization, or even standardization, in data protection standards. As personal data are universally collected and shared across sectoral and national boundaries, inconsistent data protection laws pose increasing threats to individuals, institutions, and society.

Perhaps the greatest impact of big data is the pressure it brings for new thoughtful, informed, multinational debate about the key principles that should undergird data protection. Most data protection laws continue to rely on the 1980 OECD Guidelines. The Guidelines have weathered the intervening three decades well, but it is important to remember that they were crafted not merely before big data, but also before the World Wide Web, portable laptops, GPS, smartphones, tablet devices, or the myriad other innovations that make big data possible.

Identifying common principles to undergird data protection laws is critical not only to harmonizing those laws, but also to ensure that they serve worthwhile and appropriate ends. Big data highlights the need to focus not only on 'what' and 'how', but also on 'why'. For example,

2 Kathleen M. Sullivan, 'Under a Watchful Eye: Incursions on Personal Privacy' in Richard C Leone and Gregory Anrig (eds), *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (The Century Foundation, New York 2003) 128, 131.

3 Article 44(1)(h).

- Are there limits as to what can be done with accurate, lawfully obtained information? Do they apply across the board, even to anti-terrorism and law enforcement activities? Focusing on use takes on new importance as technological applications lessen the role of law in regulating collection and sharing.
- Should there continue to be a 'Collection Limitation Principle' in a world of ubiquitous data and an apparently insatiable willingness of the public to supply its data online and off?
- Is privacy implicated if the government or a business looks at, but does not act on, lawfully obtained data, for example, when matching passenger lists with databases of suspected terrorists?
- Is there a proper role for individual consent? We believe the answer is clearly yes, but determining the contours of that role in a world of big data is not proving easy.
- Should there be a right to be forgotten—to have lawfully collected data deleted at the direction of the data subject? What does that even mean in a world of big data? Deleting data is easy, but stopping it from reappearing from another source is much harder. How do we balance the effort to do so with shared national commitments to freedom of expression?
- What is the proper and practical role for government in the face of a deluge of digital data? The sheer volume of personal data suggests that government must establish in law basic rights and obligations, but how are these to be enforced given the imbalance in resources? How do governments or independent regulators exercise meaningful oversight of the more than 60 billion credit and debit card transactions, 90 trillion emails, 1.4 trillion Internet searches, and vast number of other data transfers that occur every year?
- Governments are also among the largest collectors and users of personal data. Indeed, the advent of big data has already shown signs of marking a feeding frenzy among government agencies wanting extraordinary access to information to identify money laundering and terrorist financing transactions, locate suspect offenders, identify and block child pornography or other regulated expression, enforce intellectual property laws, or just alleviate the administrative burden of governments. A recent example of an ambitious approach to online intelligence gathering is an expression of interest by the Strategic Information and Operations Center of the US Federal Bureau of Investigations ('FBI SIOC') in developing a 'social media alert, mapping, and analysis application solution'. Among many other things, FBI SIOC would like to '[g]eo-spatially locate bad actors or groups and analyze their movements, vulnerabilities, limitations, and possible adverse actions'. Beyond that, the application might enable FBI SOIC to '[p]redict likely developments in the situation or future actions taken by bad actors . . .'.[4]
- Do we need to rethink the concept or the application of national sovereignty in the context of inherently global data flows? As European Data Protection Supervisor Peter Hustinx noted in 2007: 'Whereas the jurisdiction of the Community legislator is limited to the territory of the European Union, the external borders become less relevant for data flows. The economy depends more and more on global networks. . . . In general, the physical place of a processing operation is less relevant.'[5]

International Data Privacy Law exists in large part to help facilitate a thoughtful, informed, multinational debate about the principles to undergird society's responses to these and other data challenges. In the pages that follow in this issue and future issues, our contributors not only address ways of improving data protection in the face of big data, but also remind us of the vital need to work together to identify the principles that should guide our efforts.

doi:10.1093/idpl/ips003

4 'FBI releases plans to monitor social networks', *New Scientist*, One Per Cent Blog, 25 January 2012, available at <http://www.newscientist.com/blogs/onepercent/2012/01/fbi-releases-plans-to-monitor.html>.

5 Peter Hustinx, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (25 July 2007), available at <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf>.

Journal of Business Ethics (2006) 67:107–123
DOI 10.1007/s10551-006-9007-7

Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns

Laurence Ashworth
Clinton Free

ABSTRACT. Technology used in online marketing has advanced to a state where collection, enhancement and aggregation of information are instantaneous. This proliferation of customer information focused technology brings with it a host of issues surrounding customer privacy. This article makes two key contributions to the debate concerning digital privacy. First, we use theories of justice to help understand the way consumers conceive of, and react to, privacy concerns. Specifically, it is argued that an important component of consumers' privacy concerns relates to fairness judgments, which in turn comprise of the two primary components of distributive and procedural justice. Second, we make a number of prescriptions, aimed at both firms and regulators, based on the notion that consumers respond to perceived privacy violations in much the same way they would respond to an unfair exchange.

KEY WORDS: Digital privacy, fairness, online behavioural marketing, theories of justice

Laurence Ashworth is an Assistant Professor at the Queen's School of Business, Queen's University, Canada and received his PhD from the University of British Columbia. Dr Ashworth is interested in social and affective influences on consumer judgment and decision making.

Clinton Free is an Assistant Professor at the Queen's School of Business, Queen's University, Canada and received his D Phil from Oxford University where he was a Rhodes Scholar. His research is primarily in the areas of management control, supply chain accounting, customer accounting and the legal environment of accounting and management. Prior to obtaining his PhD, Dr Free worked for a major accounting and law firm in Sydney, Australia.

Introduction

– AT&Ts reputed first ever "You Will" Internet banner advertisement in 1994.

Not even the self-assured designers of the first-ever banner advertisement could have foreseen the way in which rapid advances in information technology over the past two decades have dramatically reduced the cost of gathering and analysing consumer information. Although initial forecasts of business to consumer (B2C) internet trade have proven largely over-inflated, the growth in online consumer sales in recent years has been striking. The widespread acceptance of the Internet as a platform for commerce has made it possible for organisations to gather a wide range of consumer information including browsing patterns, items purchased, profitability, dates and times of activities and keystroke behaviour. Drawing on the richness of this data, over the past decade online behavioural marketing, which uses browsing behaviour as a predictor of receptiveness to certain ad messages, has burgeoned. Concomitant with this growth has been an escalation in privacy concerns relating to the collection and use of information gathered online (so-called online "dataveillance"[1]) (Caudill and Murphy, 2000; Miller and Weckert, 2000).

The marketing industry has long been a cause célèbre of privacy advocates. Certainly, tracking consumer spending patterns, movements and preferences are not new marketing phenomena. However, in the online environment, privacy issues are fundamentally different in terms of scope and nature.

The technologies of e-commerce allow companies to access consumers in ways that do not involve the sorts of physical transactions that have been seen as paradigmatic of definitions of traditional privacy and property. Palmer (2005) argues that the underlying privacy issues relating to online activity transcend traditional "questions of product" to invoke "questions of technique," that is, questions involving the means by which a "business interacts with its consumers or potential consumers rather than on the nature of the product or service itself or the message put out about that product." Online marketers have the ability to access information about consumers in a way that consumers can neither avoid nor detect. Cookies, spyware, adware and online forms can covertly capture a broader, richer set of data at a lower cost than is possible under more traditional forms of customer surveillance such as point-of-sale information. Indeed, in a recent survey, 80% of respondents were found to have some form of spyware on their computer (though 95% of respondents claimed that they had not granted permission for installation) (America Online and National Cyber Security Alliance, 2004).

Privacy has consistently been identified as a chief concern of Internet users throughout the past decade (see Palmer, 2005; Petrison and Wang, 1993). Regulators and governments have implemented a wide range of responses in an attempt to balance the interests of various online stakeholders. Table I provides an overview of the state of current regulation approaches throughout the world. Regulatory responses are anchored by two positions: either governments should proactively protect consumer rights or online users should be granted the right to manage their own privacy in concert with corporate self-regulation (see Bennett, 2004 for a review). In broad terms, the argument for direct government legislation is that it increases consumer confidence and therefore increases commerce. Those supporting self-regulation counter that legislative regulations interfere with the workings and integrity of the free market and that the less formal processes of self-regulation make it more flexible and therefore less likely to stifle innovation or excessively limit consumer choice. These positions are underpinned by two contrasting assumptions about consumer behaviour: either consumers have an unalienable right to privacy that requires blanket protection or they are rational calculators capable of acting in their own interests with minimal protection.

The purpose of this paper is to provide a more robust, psychologically informed understanding of consumer conceptualisations of privacy concerns. It is argued that a more comprehensive understanding of the way consumer's understand, and react to privacy concerns will facilitate a more informed and balanced debate about digital privacy. This paper is structured in six main sections. The next section briefly overviews the emerging literature dealing with privacy issues in the online environment and introduces some of the psychological components of privacy concerns. Drawing on established psychological theories of justice, we then develop a model to help understand the way in which consumers conceive digital privacy concerns and react to various forms of online dataveillance. Using theories of justice to understand consumers' online privacy concerns develops the implications of various components of justice theory and puts forward a set of propositions to attend to consumer perceptions and likely online behavioural responses. Placing primacy on consumer empowerment rather than corporate restraint, we argue that appropriate privacy policies have the potential to provide a basis for competitive advantage and that major online players, such as Microsoft, Yahoo and Google, have a crucial role to play in responding to consumer privacy concerns. Finally, we suggest a number of fruitful avenues for future research and conclude the paper.

Background

In recent years, three broad streams of research have begun to examine some of the ethical and legal issues relating to online marketing, and e-commerce more broadly. In the first, an eclectic mix of ethical lenses have been applied to the issue including utilitarianism, egoism, moral relativism, duty-based theories and social contract theory (Caudill and Murphy, 2000; Miller and Weckert, 2000; Sarathy and Robertson, 2003). A separate stream of research has focused largely on examining how various individual and organisational level variables influence organisational attitudes and actions towards privacy. For example, researchers such as Sarathy and Robertson (2003) have examined how managerial attributes and

TABLE I

An overview of regulatory approaches across the globe

Approach	Description	Exemplar
Legislative responses		
The "US approach"	Privacy conceived primarily as a commodity controlled through the free-market with protection focused on narrow categories of sensitive data, such as data held by financial institutions and data relating to children	Children's Online Privacy Protection Act (1998)
The "EU approach"	All member states of the European Union are required to protect the "fundamental right" to privacy of individuals and restrict the transferring of data to countries that do not ensure an equal level of protection.	Directive 95/46/EC of the European Parliament (1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data
Self-regulatory or market-based responses		
Privacy standards	A set of mandatory criteria and/or voluntary guidelines designed to promote privacy best practices across industrial sectors, nations, or regions.	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
Privacy codes of practice	Rules and procedures designed to govern information collection within specific organizations or groups	Sun Microsystems Privacy Policy (http://www.sun.com/privacy/)
Third party entity certification and privacy seals	Independent third party entities issuing licenses and proprietary privacy seals with respect to privacy practices.	Truste, BBBOnline and the Online Privacy Alliance
Technological solutions	Privacy-enhancing technologies allow consumers direct control of the information on their computer. They include cookie managers, ad-blockers, encryption software, and clean-up tools.	Zero Knowledge Systems Pop-Up & Ad Blocker System
The market mechanism	A number of websites now make it possible for a willing consumer to trade some aspect of privacy as part of the transaction for goods or service.	The Central Texas Mortgage Corporation (CTMC) offers entry into online contests and sweepstakes in return for personally identifiable information
Consumer activism	A policy of taking direct action in online and offline environments to achieve desired enhancements in privacy policy	The American Civil Liberties Union's "Take Back Your Data Campaign"

organisational contextual factors such as ownership, information intensity, age and e-commerce experience influence managers' preferences regarding privacy procedures. At the other end of the spectrum, researchers have sought to determine the way in which personal characteristics such as gender, race and Internet experience are associated with privacy concerns among consumers (Chen and Rea, 2004; Milne et al., 2004). For example, Chen and Rea (2004) find a direct relationship between demographic variables (gender and racial grouping) and privacy control techniques. Finally, in a third and perhaps most mature stream of inquiry, legal scholars have described and debated the merits of various forms of cyber regulation (see, e.g. Kotzer, 2003; Bentivoglio et al., 2003).

In spite of this recent surge in research interest, consumers have been largely ignored by policy makers and researchers alike. For example, consumers' attitudes and opinions with respect to privacy concerns have been mostly unheard during the FTCs considerations and testimonies. In FTC hearings between 1995 and 2000, the only consumer voice presented was through the results of

broad-based consumer telephone polls, which reported responses to a single generic question: How concerned are you about privacy online? (Sheehan and Hoy, 2000). This single question provides no insight into what online activities consumers are actually concerned about or why these activities should trouble them. Moreover, studies of privacy adopting economic epistemology have tended to view individuals as rational economic agents who can make informed decisions regarding the protection or divulgence of personal information (Acquisti and Grossklags, 2005; Taylor, 2004). While this assumption may be analytically useful, it precludes the possibility that consumers' privacy concerns reflect something other than the results of an analysis of the costs and benefits of disclosing information online. Recent research has started to examine some of the factors that underlie consumers' privacy concerns. However, the majority of this work has attempted to identify underlying components of the construct rather than provide a theoretical framework that explains why those particular components should exist.

The psychological components of privacy: what do consumers care about?

Current research suggests that one of the primary concerns relating to privacy is the lack of the control consumers have over their personal information (Nowak and Phelps, 1995). Sheehan and Hoy (2000) argue that control consists of two dimensions: awareness of information collection and information usage. Awareness of information collection refers simply to whether or not consumers are aware that marketers are collecting information about them. This dimension of control is often discussed in relation to permission and disclosure (e.g. Cespedes and Smith, 1993; Nowak and Phelps, 1995). When online agents ask permission to collect information or disclose that they will be collecting information consumers become aware that information about them is being or will be collected. Research has shown that privacy concerns tend to be reduced when permission is obtained (Nowak and Phelps, 1995) and heightened when consumers discover information was collected without their awareness (Cespedes and Smith, 1993). This aspect of privacy concerns relates closely to what Palmer (2005) calls "questions of technique" – without permission or disclosure (neither of which are routinely practiced) information can be collected in a way that consumers can neither avoid nor detect. The second dimension of control, information usage, refers to how marketers use the information they collect. Privacy tends to be more of a concern when marketers use the information for purposes beyond the initial transaction (Foxman and Kilcoyne, 1993) or sell the information to third parties (Nowak and Phelps, 1992). Sheehan and Hoy (2000) introduced a number of additional factors that were also shown to relate to privacy concerns. These factors included the sensitivity of the information collected, the familiarity with the online entity, and whether or not consumers were compensated for the information they provided.

Hence, existing research on the dimensions of privacy has identified a number of factors that appear to underlie privacy concerns and highlighted the multi-dimensional nature of privacy as a construct. However, this literature does not provide a theoretical framework that explains why these components per se should be important to consumers. While awareness, permission and other identified dimensions of privacy do seem to be relevant to consumers' privacy concerns, it would appear that consumers are employing some other criteria when making judgments related to their privacy. Specifically, we suggest that consumers' privacy concerns actually entail an evaluation of information collection within the framework of exchange.

Information collection as exchange

Marketing interactions generally have been described under the framework of exchange (Bagozzi, 1975), and we argue that the collection and dissemination of information online can also be viewed in this fashion. That is, consumers perceive the information that is collected about themselves to be an input into an exchange with the online agent. In return, they expect to receive outcomes such as online services, goods, monetary compensation, or something else of value. Figure 1 illustrates a number of the common forms of exchange involving information about consumers that exist online.

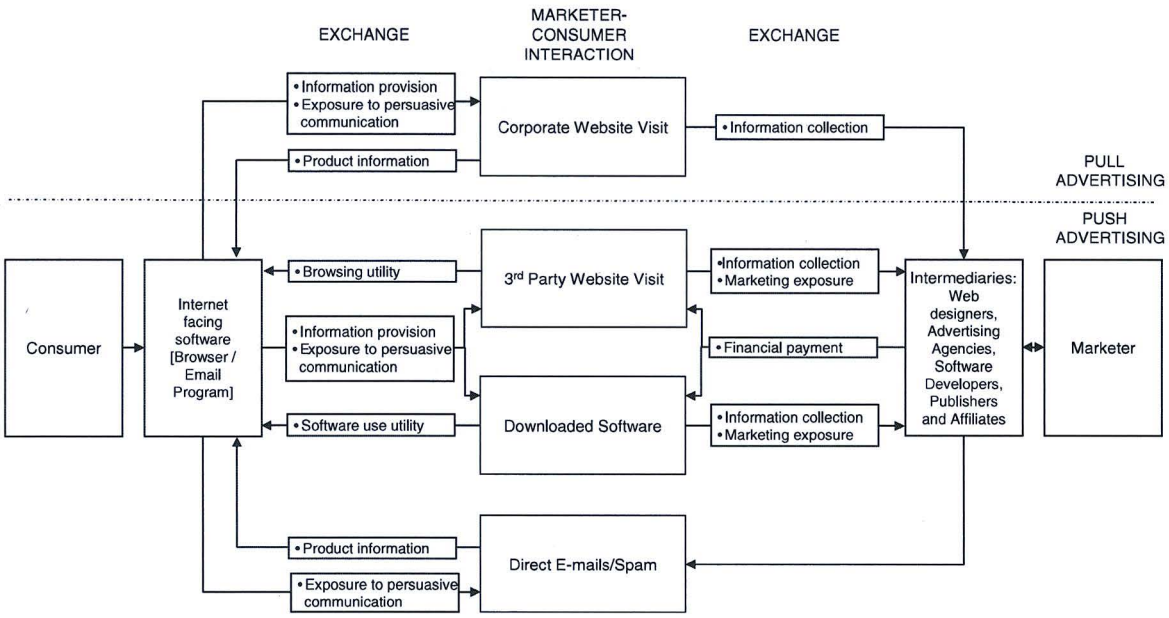


Figure 1. An exchange model of online marketing.

The diagram illustrates that, from the consumers' perspective, the online exchange is facilitated by means of internet facing software, such as a web browser, which interacts with the firm's information collection mechanism, such as their website, or software that is made available for downloading. Through these media, marketers collect consumer information in return for certain benefits. The information collected constitutes one of the consumer's inputs to the exchange and an outcome for the marketer. Consumers may provide additional inputs, for example, by being exposed to persuasive communications. Again, this would constitute a positive outcome for the marketer, at least as perceived by the consumer. In return for such inputs, consumers can receive a variety of positive outcomes, including access to a particular website, the benefits offered by downloaded software and monetary compensation. In other instances, consumers may receive no positive outcome or even a negative outcome, such as when they receive spam or provide information that they believe could be used to defraud them.

It should be noted that there are a number of assumptions and implications inherent to this framework. First, conceptualising privacy concerns as an exchange involving information collection and provision necessarily implies that consumers will only harbour privacy concerns to the extent they believe that information about them is collected online. Unlike ethical and legal examinations of privacy where the invisibility of information collection is a major point of contention, consumers should only be concerned about their online privacy to the extent they believe information is being or could be collected. Second, for consumers to consider information about themselves an input to the exchange implies they perceive themselves to have ownership of that information, consistent with existing evidence (Trurow, 2004). Finally, the exchange framework supposes that consumers perceive information about themselves to be of some value to the online agent, and therefore, a positive outcome of the exchange for the marketer. To the extent that different kinds of information are perceived as more or less valuable to marketers, consumers' assessment of the exchange and therefore their privacy concerns are likely to be affected.

One of the consequences of framing information collection as an exchange is that it suggests consumers' privacy concerns are likely to relate to two distinct facets of the exchange. The first is the possibility of negative outcomes resulting from the exchange.

That is, privacy concerns are in part likely to reflect the possibility that by engaging in an exchange involving information with an online agent, the information may be used in a manner that is harmful to the consumer. The second, related judgment is one of fairness. Fairness is an important psychological evaluation associated with exchange (Adams, 1965) and we argue that one of the reasons consumers are concerned about online exchanges involving information is that they are often perceived to be unfair. The current work is concerned with fairness as a component of consumers' privacy concerns.

We argue that fairness judgments encompass many of the different aspects of consumers' privacy concerns that have been voiced in the literature. For instance, compensation and information sensitivity (Sheehan and Hoy, 2000) can both be viewed as assessments of inputs and outcomes of an online exchange – consumers receive compensation (their outcome) for providing information (their input) and marketers receive information (their outcome) in return for compensation (their input). An important psychological evaluation of such an exchange is whether or not it is fair. That is, one reason compensation and information sensitivity are important to privacy concerns is because they form components of a fairness judgment. We proceed by providing an overview of fairness, as studied under the rubric of justice theory in social psychology, organisational behaviour and marketing. Based on this literature, we argue that privacy consists of two basic concerns: a concern for one's material outcome (which we argue is related to the motivational underpinnings of distributive justice) and a concern that one is treated as a respected and valued individual (which forms the psychological basis of procedural justice). We show that the psychological components of privacy that have been discussed in the literature fit well into the framework of exchange and justice. Finally, we attempt to demonstrate that this conceptualization of privacy can provide important insights to firms and policy makers alike.

Using theories of justice to understand consumers' online privacy concerns

The notions of justice and fairness are multidimensional and multifarious constructs that have been studied across a wide variety of disciplines including ethics, economics, sociology and psychology. Given that our focus relates to individuals' psychological evaluations and reactions to perceived injustices, we focus on the organisational and social psychological literature. Within these areas, justice has received much attention in recent years. However, opinion still differs regarding the dimensionality of the construct. There appears to be agreement that justice is comprised of at least two components, namely, distributive and procedural justice (Colquitt et al., 2001). However, some researchers have argued for a single underlying dimension (e.g. Cropanzano and Ambrose, 2001), while others have argued for a host of other components, including interactional, interpersonal and informational justice (e.g. Bies and Moag, 1986; Greenberg, 1993). This disagreement appears to stem from whether one adopts a structural or psychological perspective of justice.

Traditionally, the different components of justice have been predicated on structural differences in the context in which justice is studied. Up until Thibaut and Walker's (1975) seminal work on procedural justice, justice was primarily considered to relate to the distribution of outcomes. Thibaut and Walker, however, recognised that in dispute resolution procedures perceptions of justice were also a function of the way in which the procedure was conducted. Specifically, they noted that disputants' sense of justice was heightened by their ability to actively present their arguments or, in their language, be afforded "voice". Early researchers on procedural justice assumed that voice was ultimately important because of its potential to impact outcomes. In other words, the same psychological processes were assumed to underlie judgments of distributive and procedural justice. Thus, the two dimensions of justice reflected the two-component structure of dispute resolution procedures, but were ultimately driven by one underlying psychological mechanism.

Later researchers recognised that perceptions of justice might be related to more than just concerns about the final outcome. Specifically, Lind and Tyler (1988) argued that procedures also convey the extent to which individuals are respected and valued members of an organisation, which they called the relational or group-value model of procedural justice. There is now widespread agreement that

respect is integral to procedural justice (Miller, 2001) because procedures are particularly apt at conveying respect relative to outcomes (Vermunt et al., 2001). It has been further recognized that respect can be conveyed directly via the interpersonal communication of procedures (rather than *implied* by particular procedures). Bies and Moag (1986) argued that this should be considered a distinct component of justice, which they labelled interactional justice. Others have argued that interactional justice itself consists of two components: informational and interpersonal justice (Colquitt et al., 2001; Greenberg 1993). Informational justice refers to the fact that part of the importance of interactional justice stems from explanations of the procedures used to determine outcomes. Interpersonal justice captures the respect conveyed during the social interaction and is therefore comparable to the original definition of interactional justice.

Thus, in the psychological literature, arguments have been made that justice consists of anywhere between one underlying dimension (Cropanzano and Ambrose, 2001) and up to four (Greenberg, 1993). Despite these disagreements, the various components of justice appear to reflect two underlying concerns – a concern that one is treated with respect and a concern for one's material outcome. Within the literature there is widespread agreement that judgments of distributive justice tend to reflect material concerns, while judgments of procedural justice are motivated primarily by concerns for the way one is treated. We have argued that the other components of justice in the literature reflect the same underlying concern as that voiced for procedural justice, namely respect. Consequently, the current work focuses on distributive and procedural components of justice and treats each as though they are tantamount to the two psychological concerns described.

Distributive justice

Distributive justice relates to the perceived fairness of the allocation of outcomes and is assumed to reflect a concern for one's material well-being. Outcomes can be based on a number of possible criteria, including merit, need, rights and duties (Deutsch, 1985). For example, according to equity theory (Adams, 1965) distributive justice is based on a comparison of the ratio of one individuals' outcomes and inputs to another's. A fair allocation would therefore require each individual's outcomes to be in proportion to the inputs they have contributed. In a marketing context, transaction utility theory (Thaler, 1985) suggests that consumers engage in a similar comparison process to determine the fairness of a price. Consumers compare the price they are offered or have paid to some reference price for the good. Prices that are greater than the reference price are considered unfair, while prices that are equal to or less than the reference price are considered fair. While there are a number of different theories of distributive justice, they are fundamentally comparative in nature – individuals are assumed to compare their outcome to some referent standard that they believe they are entitled to. Outcomes that are considered inferior to the referent standard lead to perceptions of distributive injustice.

Procedural justice

Under the traditional definition, procedural justice refers to the fairness of the rules or policies that are used to allocate outcomes (Leventhal, 1980; Thibaut and Walker, 1975). This facet of justice has been most extensively studied in an organisational context. Research has demonstrated that the fairness of procedures can be more important than outcomes when it comes to predicting a number of important organisational variables. For example, Folger and Konovsky (1989) have demonstrated that the procedures used to determine pay raises were of similar importance to the actual raise when it came to satisfaction, and more important when it came to organisational commitment and trust in the employees' supervisor. As discussed, one important reason individuals care about procedures is because they are particularly apt at conveying respect and value. This perspective is known as the group value or relational model of procedural justice (Tyler and Lind, 1992) and it is this that distinguishes the psychological basis of procedural justice from distributive. According to this perspective, a procedure should be considered fair to the extent that it communicates to relevant individuals that they are valued and respected members of the organisation.

In short, the research on justice suggests that there are at least two broad psychological processes that underlie justice judgments. The first relates to whether or not an individual receives an appropriate outcome based on some relevant criteria (distributive justice). The second relates to whether or not an individual is treated in a manner that communicates they are respected and valued (procedural justice).

Privacy concerns and distributive justice

In the context of online privacy, consumers are likely to have concerns that relate to both procedural and distributive facets of justice. Judgments of distributive justice reflect consumers' evaluations of the fairness of the allocation of outcomes. Such judgments are comparative in nature and entail an assessment of both consumers' and firms' outcomes and inputs (Walster et al., 1973). This is consistent with the notion that information collection is part of a multifaceted exchange between consumers and firms. Within the exchange, both parties receive a variety of outcomes and contribute a variety of inputs. For example, drawing on the online exchange model in Figure 1, a typical exchange might consist of the provision of personal information (which would constitute the consumers' input and one element of the firm's outcome) in exchange for access to a Web page or software (which would constitute one element of the consumer's outcome and part of the firm's input). There are, of course, other outcomes and inputs. For example, the consumer may also believe they are more likely to receive unsolicited e-mails, which would represent a negative outcome for the consumer and, potentially, a positive outcome for the firm. The exchange relationship and examples of relevant outcomes and inputs are shown in Figure 2.

According to equity theory (Adams, 1965), perceptions of distributive justice are the result of a comparison between (a) the consumer's outcomes relative to what they contributed to the exchange in the form of inputs, and (b) the firm's outcomes relative to their inputs. A distributively fair solution requires that consumers' outcomes and inputs be in the same proportion as the firm's or, that $\frac{\text{Outcome}_{\text{Consumer}}}{\text{Input}_{\text{Consumer}}} = \frac{\text{Outcome}_{\text{Firm}}}{\text{Input}_{\text{Firm}}}$. From the consumer's

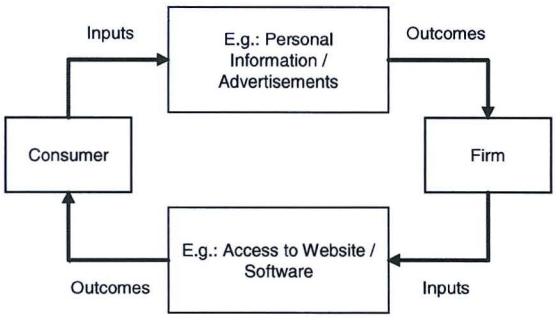


Figure 2. Consumers' and firms' inputs and outcomes of exchange.

perspective, this means that the rewards for providing personal information should be commensurate with the perceived value of the information to the firm relative to the costs incurred by the firm to obtain that information. This framework could help to explain why consumers find it unacceptable for marketers to sell their personal information, regardless of the intended use (Nowak and Phelps, 1992). The sale of the information represents an additional positive outcome for the firm that they are not entitled to without a corresponding increase in consumers' outcomes (or decrease in their inputs). In fact, it could even represent an additional negative outcome for consumers if they believe they will be subject to more spam or increased risk of fraudulent activities. Cast either way, such perceptions are likely to create or exacerbate perceptions of inequity.

It should be noted that judgments of distributive justice do not preclude the likely possibility that consumers will conduct an independent assessment of their outcome. This, we would argue, is also an important facet of privacy concerns – outcome *favorability*. Outcome favourability refers to whether one receives a positive rather than a negative result (Kulik and Ambrose, 1992). Research on justice has generally conflated outcome favourability and outcome fairness, based on the argument that there is little distinction between these two constructs (e.g. Brockner and Weisenfeld, 1996). It is not clear, however, that favourable outcomes are necessarily fair or that unfavourable outcomes are necessarily unfair. Although consumers do tend to be more concerned with the fairness of unfavourable outcomes (Deutsch, 1985), even favorable outcomes can be perceived negatively when they are

considered unfair – a finding originally termed relative deprivation (Homans, 1961). Consistent with this, Adams (1965) also predicted that individuals would be likely to have a higher tolerance for advantageous inequity (unfairness in one's favour) than disadvantageous inequity. In the context of online exchange then, this suggests that consumers will judge both the fairness of their outcome, a judgment that is likely to involve both consumers' and firms' outcomes and inputs, and the value of their own outcome, a judgment based purely on the merits of what it was they received.

There is further evidence that suggests consumers' assessment of their outcome is likely to be strongly influenced by negative components of the outcome (e.g. the possibility of recurring spam or identity theft after an online exchange of information). Although some components of consumers' outcomes are likely to be positive (e.g. access to software or the content of a website), losses tend to loom larger than gains (Kahneman and Tversky, 1979), meaning that consumers may be focused on the negative elements of their outcome. Moreover, negative outcomes tend to be probabilistic (e.g. the *probability* of having one's identity stolen or of receiving spam), and probability judgments are subject to certain biases, such as overestimating the probability of events that are easy to recall and the over-weighting of low probabilities (Kahneman and Tversky, 1979). Such biases are likely to exacerbate the effect of negative outcomes. As such, the outcome component of consumers' privacy concerns should be disproportionately influenced by the possibility of negative consequences.

Privacy concerns and procedural justice

Research on procedural justice indicates that the extent to which individuals are treated in a respectful manner is a second important determinant of justice perceptions. The work of Miller (2001) suggests that one way in which individuals make such judgments is by comparing their treatment to normative standards of respectful behaviour. Such standards are known as prescriptive norms (Cialdini and Trost, 1998) and can vary considerably according to the social situation. In the context of online privacy it seems likely that there are a number of standards that would indicate consumers are respected and valued. Violations of these standards are predicted to lead to perceptions of procedural injustice, which will create the impression that the firm has acted unfairly in the exchange.

It is likely that a number of normative standards exist that is relevant to the collection of personal information online. For instance, consumers may hold a norm of *openness*, which would dictate that information collectors should provide consumers with a clear and unambiguous description of all information that is collected as well as the intended uses of that information. Consistent with this, internet users have indicated that they would be more willing to provide information to the extent that firms provide an explanation of how that information will be used (Trurow, 2004). Moreover, there is survey evidence that consumers are distrustful of legalistic disclosure documents (OECD, 2003), perhaps because they appear to deliberately mask firms' information collection policies.

There may also exist a norm of *information access*, which would dictate that information collectors should allow consumers' ready access to the information collected and furthermore, provide consumers with the ability to change or delete that information. Allowing consumers to view, update, change or delete information about themselves communicates that the consumer is suciently respected and valued that they should be aorded complete control of the information. It is possible that consumers hold the belief that they have a fundamental right to their personal information (Trurow, 2004), in which case, adhering to a norm of information access may not convey respect per se. However, violation of the norm would most likely communicate disrespect.

Another norm that consumers may hold is a norm of *permission*. This would require that information collectors ask for consent before they collect even the most innocuous information. In certain instances, it may seem trivial to ask for permission for data that is freely available and unlikely to be considered sensitive. However, doing so communicates that the consumer's preferences are respected and, by extension, that the consumer is valued. This is a message that can be conveyed even when the nature of the data does not warrant obtaining permission. Finally, it should be noted that there is probably a

broad norm of *honesty* operating in all these instances, which would dictate that information collectors should be truthful and avoid deception.

This list of normative standards is not intended to be exhaustive, however, it is designed to represent the principal kinds of normative expectations that consumers might have of online information collectors. These normative standards are reflected in a variety of guidelines articulated by a number of different regulatory bodies. For example, in 1998 the FTC established five principles that relate to the normative standards outlined in the previous paragraph. They include (i) provision of notice/awareness of information collection, (ii) obtaining consent and providing consumers with a choice, (iii) providing access to the information collected and participation rights, (iv) integrity/security and (v) the necessity of mechanisms for enforcing the guidelines and providing redress in case of violations. The OECD proposed similar guiding standards in 1980 (OECD, 2003), including limits to the collection of data; that data should be accurate and relevant; that the purpose should be specified; limits on the use of the data; safeguards for the security of the data; openness of information regarding the data collected and the data controller; individual rights to view and change data; and finally, that data controllers should be accountable to the aforementioned standards. Such guidelines readily map onto (and in some instances might exceed) the kinds of normative standards that consumers might hold information collectors to.

In most situations, a violation of one of other of these normative standards is likely to affect consumers' perceptions of the outcomes and inputs of the exchange as well. For example, a violation of the norm of permission might lead consumers' to infer that they are more likely to be defrauded or spammed. However, it is specifically argued that the violation exerts an independent influence on perceptions of justice, regardless of whether there are any tangible consequences. To illustrate, consider a hypothetical situation where a consumer is assured, by virtue of their technical expertise, that disclosure of their personal information will lead to no harmful consequences. Now imagine that a company attempted to collect information without obtaining their permission beforehand. Will this be considered an injustice? According to the justice framework developed in the current paper, it will – because the firm violated an important interpersonal standard, which will lower perceptions of procedural justice.

Justice and the dimensions of privacy

The conventional understanding of online privacy concerns in marketing is that they consist of two dimensions: awareness and usage of the data outside of the original context (Nowak and Phelps, 1995). It has been suggested that privacy concerns may also entail an assessment of information sensitivity, trust and familiarity with the information collector, and compensation (Sheehan and Hoy, 2000). According to the justice perspective developed in the current paper, two factors underlie such assessments: distributive and procedural justice. Information sensitivity, data usage and compensation are directly relevant to judgments of distributive justice; although information sensitivity and data usage may also affect perceptions of procedural justice as we shall see. Awareness is hypothesised to be primarily of importance to judgments of procedural justice through its relation to the norms of permission and notice. Trust, we hypothesise, is an important moderator variable that is likely to influence the inferences consumes make about elements of both procedural and distributive justice.

Information sensitivity is likely to affect perceptions of distributive justice by influencing perceptions of the inputs and outcomes involved in the exchange. First, the collection of sensitive information is likely to reduce consumers' outcome of the exchange because the potential consequences associated with the collection of sensitive information are more severe than the consequences associated with less sensitive information. Second, sensitive information may well increase consumers' evaluation of their input to the exchange as they are now providing information they perceive to be more valuable. By the same token, consumers are likely to believe that the firm receives information that is more valuable and therefore that their outcome has increased. Within the context of the equity equation, all of these changes work in concert to alter the equity equation in favour of the firm, thereby lowering perceptions of distributive justice.

Information usage also factors into the equity equation by affecting perceptions of the firms' outcome. For example, selling information to a third party should raise consumers' evaluation of the firms' outcome as the exchange has now yielded the firm an additional positive outcome. Selling information may also lower consumers' own outcome due to perceptions that they are at greater risk of negative consequences. Again, such evaluations will likely lower perceptions of distributive injustice. Compensation fits into the equity equation in a similar fashion – it constitutes one element of consumers' outcome and another element of the firm's input. Thus, by providing even meagre compensation firms can raise consumers' outcome and increase perceptions of their own input, helping reduce perceptions of distributive injustice.

Information sensitivity and data usage may also impact perceptions of procedural justice depending on the procedures associated with each. For example, use of the data that goes beyond the original stated purposes (assuming consumers discover or suspect such use), violates both norms of permission and notice. Consumers were neither asked if the data could be used in that way nor informed prior to collection. Thus, the inappropriate use of data is likely to lower perceptions of both distributive and procedural justice, but for different reasons. Although the collection of sensitive information might run into the same procedural problems, it is possible that consumers object to the collection of any information deemed too personal, regardless of the intended use. As such, information sensitivity, for some individuals, may represent an additional procedural norm that cannot be violated within the context of exchange.

Awareness of information collection, as described within the research on the dimensions of privacy, most likely relates to information collection and use that violates the norms of permission and notice discussed previously. That is, awareness per se is not important to consumers (except in the sense that consumers must be aware of information collection before they can subsequently evaluate the exchange), but rather, the current framework suggests that it is the violation of norms of permission and notice, which are likely correlated with awareness, that consumers react to. In contrast, while adherence to each of these norms creates awareness, again, it is the observation of the norm that is likely to raise perceptions of procedural justice rather than awareness itself.

Finally, trust is likely to act as a moderator variable that influences both types of justice judgments through its effect on the inferences consumer make regarding the components of the distributive and procedural justice judgments. In terms of distributive justice, trust in an online agent is likely to affect consumers' inferences about the inputs and outcomes of the exchange when they have incomplete information, such that the exchange is more likely to be perceived as distributively fair, and therefore privacy concerns are likely to be reduced. Trust may well moderate inferences regarding the violation of procedural norms as well. For instance, in the case of data usage, consumers who trust an online agent may be more likely to infer that data will not be used beyond the original purpose when they have not received explicit information to this effect. Consequently, perceptions of procedural injustice are likely to be lower than for an online agent that is not trusted, as consumers may well assume the data will be used outside of the original context. Finally, trusted entities may well be held to higher standards of normative adherence. Ironically, this means that a normative violation by a trusted agent might convey more disrespect than a violation by an unfamiliar firm, lowering procedural justice and increasing privacy concerns.

In summary, it is proposed that the conventional understanding of the dimensions of online privacy can be explained within the framework of justice theory. The justice framework suggests that consumers may attend to two separable and distinct components. On the one hand, they are likely to evaluate the fairness of the distribution of outcomes, which includes the tangible consequences of the information collection to both themselves and the beneficiaries of the information. On the other hand, they are likely to evaluate the fairness of the manner in which they were treated, by comparing their treatment to normative standards of respectful treatment. Both judgments are comparative in nature. However, judgments of distributive justice involve a relative comparison, whilst judgments of procedural justice involve a comparison to an absolute standard.

Discussion

The justice framework underlines the importance of consumer responses to the procedures and outcomes of incursions on consumer privacy. The first part of this section draws a set of implications that are relevant to organisational policy making in the online context. These propositions provide a platform for a focused discussion of two further prescriptions. The first is that firms should consider privacy policy a strategic resource to be proactively managed. The second is that procedural advances that effectively empower consumers are particularly welcome.

Implications of a justice framework for policy

The primary implication of this framework is that one of the ways in which consumers' privacy concerns will manifest themselves is in a fairness judgment that is derived from both consumers' and firms' outcomes and the manner in which personal information is collected online. This framework raises a number of questions and points that have been overlooked in other analyses of online privacy issues. First, the emphasis of this framework is on consumer evaluations of privacy rather than on the public policy or legal issues that surround online privacy concerns. The implication is that firms and online information collectors need to be aware of consumers' evaluations – both in terms of outcomes and procedures - of their online business practices, as this is likely to be a source of negative consumer behaviour, including boycotts, negative word of mouth (including dissatisfaction voiced through weblogs, discussion boards, chat rooms and dedicated websites), complaining and even attempts to punish firms that are perceived to have acted unfairly. Conversely, online practices that are considered fair may well build trust and encourage consumers to engage in more online transactions. For example, compensation works as an automatic announcement to users that information is being collected, which, research finds, eliminates some consumer privacy concerns up front (Milne and Gordon, 1993). Thus, firms cannot simply view online information collection as something to be conducted within the bounds of existing legislation. Instead, they need to consider consumers' reactions to their online policies if they are to maintain and build profitable customer relationships.

The fairness framework expounded in the current paper also highlights a number of variables that consumers are likely to attend to. For instance, when it comes to judgments of distributive justice, equity theory predicts that consumers will consider their outcomes and inputs and their perceptions of the firms' outcomes and inputs. These are subjective judgments and in the absence of veracious information consumers will most likely rely on their own attitudes and beliefs to form a judgment. This opens the door for potentially biased judgments. For example, when it comes to judging their own outcomes, consumers may overestimate the negative consequences associated with the collection of personal information (e.g. the number of spam e-mails). They may also overestimate the benefits to the information collector of the information that is collected. Misjudgments such as these will only exacerbate consumers' perceptions of distributive injustice. The implication is that firms will be better off providing consumers with concrete, detailed information relating to both the likely consequences for consumers as well as the benefits to the firm of the information collection. Such openness should reduce the possibility that consumers will form biased judgments and, moreover, will likely have implications for consumers' perceptions of procedural justice as well.

The current analysis suggests that perceptions of procedural justice reflect the extent to which prescriptive norms of openness, information access, permission and honesty are observed in the collection of information online. In many situations the violation of prescriptive norms is likely to coincide with perceived consequences. For example, failing to disclose the use of information collected online not only represents a violation of an openness norm, but may also exacerbate consumers' perceptions of the negative consequences that could stem from the information collected. Indeed, consumers' privacy concerns are likely to increase as they become aware that marketers have somehow obtained information about them without their awareness or permission (Cespedes and Smith, 1993). Similarly, unsolicited e-marketing approaches compromise norms surrounding permission. To this end, research from the direct mail marketing literature (Rogers, 1996)

suggests that people are more likely to look at mail sent by businesses they know and with whom they have done business.

Although the effect of the normative violation and the belief that negative consequences will ensue are confounded, they do represent different judgments according to the justice framework. In particular, we argue that a normative violation alone, even when consumers perceive the information collection to be distributively just, will inspire perceptions of procedural injustice which will lead to negative behaviours and attitudes similar to those we would expect in response to a distributive injustice. Thus, firms cannot just consider the tangible outcomes associated with the collection of personal information when it comes to predicting consumers' reactions, they also need to consider whether their procedures are violating a potentially broad array of prescriptive norms. As consumers become more IT savvy, it may be the case that consumer apprehensions of justice will become more exacting. A recent experimental economics study concluded that there are two major motivating forces that drive consumers to seek sanctions (Falk et al., 2005). The first is where the consumer feels that the fairness principle has been violated (although the nature of fairness was not elaborated). The second is spite. This finding corroborates a survey on privacy by The Pew Research Center, which found that users were in a "punishing mood" (2000).

Privacy protection as a strategic asset

Over the past few years, the norms governing personal data interactions between consumers and websites have changed. There is an increasing sensitivity regarding the commercial collection and use of data; for many, the social meaning has changed from a morally-neutral to a morally charged status. Hetcher (2001) presents an actor network analysis of the way in which interested actors, such as privacy activists, the Federal Trade Commission and creators of new privacy software solutions, have deliberately and skilfully supported an entitlement to privacy. As consumers increasingly perceive an entitlement, there is a corresponding tendency for them to feel moral outrage at websites that fail to respect data privacy. The justice framework provides a rigorous device to consider privacy concerns from the consumer's perspective and suggests that relative outcomes (in terms of relative inputs and outputs) and the observation or violation of norms in privacy procedures are paramount. Consumers who feel that they are disrespected may seek to punish websites by taking their business elsewhere, reciprocating the disrespect by providing the website with false personal information, or sanctioning the website through negative online and offline gossip.

For websites at the margin, it may now make sense to switch to more respectful practices. Recent survey results suggest that it is likely that concerns relating to privacy are at least partly responsible for consumers' unwillingness to transact over the internet. In a survey of 214 online shoppers, Ranganathan and Ganapathy (2002) found that concerns about privacy had the single greatest effect on the purchase intent of online consumers. The lobbying savvy of organizations like the Electronic Privacy Information Center, the coercive power possessed by the FTC in the US and the potency of privacy software solution providers are powerful shapers of public norms regarding online privacy and appear destined to gain further momentum. Moreover, consumers are becoming increasingly familiar with internet technologies and the details of the collection and aggregation of the personal information that is collected. As consumers become more knowledgeable, not only do they have the tools to evaluate the fairness of the information collection, but they also have the tools to discriminate against the perceived offenders. Thus, the costs associated with information collection are likely to go well beyond the costs of simply collecting information.

When viewed in this way, firms need to recognise that the collection of information online can neither be treated as a low-cost method of market research nor as a fundamental right to information that is easily obtainable by virtue of current technology. There is no question that the information available over the internet is potentially an extremely valuable resource for marketers. However, the value of that information must include some consideration of consumers' reaction to the collection of personal information. The justice framework suggests that firms should explicitly stress both the categories of information that they will be collecting and the way in which the information will be utilised.[2]

Moreover, firms should be especially careful to observe the prescriptive norms that are likely to govern the collection of personal information over the internet. Moving forward, business interests rather than legal or quasi-legal rules will demand that firm's respect consumers' privacy concerns.

Consumer empowerment and digital libertarianism

Problems beset both top-down and self-regulatory solutions. We suggest that a greater focus should be afforded to empowering consumers in concert with continued reliance on the market mechanism. At present, the average consumer typically relies on a combination of third-party information protection software, assurances from a number of different privacy seals, government regulation, disclosure statements and finally firms' integrity to control the personal information that is collected online. Even in combination, these measures appear to be deficient in important respects. Instead consumers need to be empowered with the information to make an informed decision and the technological ability to control the flow of information from their computer. The first element of this empowerment requires that consumers be told in the simplest possible terms whether and what information will be collected. Standard disclosure statements typically consist of a copious quantity of complex legal jargon that neither inform nor reassure consumers that their privacy will be protected. Consistent with this, the European Union's committee of data privacy commissioners (the "Article 29 Working Party") has adopted a plan to create corporate privacy notices that are easy for consumers to understand and compare to notices of other companies.

The second element of empowering consumers involves providing them with the means to control the flow of information from their computers. Although there is a variety of third-party software solutions available, they are costly and differ in the range of information protection features that they offer. Moreover, consumers have proven slow to adopt new initiatives without the backing of large, powerful governmental or private organizations. While increased awareness and technical proficiency amongst users may dissipate this inertia, it remains the case that consumers are more likely to place their trust in solutions provided by credible third parties to protect them rather than expend the time and energy to make choices suitable to their best interest. Accordingly, private players with high levels of trust such as Microsoft, Yahoo and Google potentially play a more important role in the privacy puzzle than any individual, government body or authority.

A system that has been set up around this notion is the Platform for Privacy Preferences or P3P. It is backed up by the Online Privacy Alliance, a consortium of almost 50 American organizations including the US White House, Microsoft, America Online and organizations like the Center for Democracy and Technology. P3P uses a protocol developed by World Wide Web Consortium's (W3C) called Platform for Internet Content Selection (PICS). In its conception, PICS was designed to carry labels that would describe its content to users. Under the PICS protocol, the website owner would state the privacy level of the site. As a result, most browsers, including the dominant Internet Explorer, now feature a number of privacy protection features.

However, results to date have proven largely disappointing. Controls presented are frequently buried within the many features of the software; and high levels of "security" often interfere with the functionality of many websites (not because they are attempting to extort information, but because they use many of the design features that can be used to do so). Either browsers need to better distinguish sensitive information from information that is used simply to navigate through a series of web pages, or standards need to be introduced that separate navigation information from personal information. While a detailed technical solution is beyond the scope of this paper, it is proposed that regulatory attempts that focus on empowering consumers with the ability to control what information leaves their computer, for example, through their web browser, are preferable to those attempting to limit marketers' information collection activities online.

Future research

Theories of justice from psychology provide a useful and robust framework for further research in the area, however a number of empirical questions

remain unanswered. Specifically, further research into three specific questions is welcome.

First, while this article sets out a theoretical framework for investigating privacy issues, it requires empirical validation. The justice framework would provide a strong theoretical foundation for experimental and survey work in the area of digital privacy.

Second, methods of measuring both the costs and benefits of online behavioural marketing remain elusive. Future research considering performance measures capturing the financial benefits, as well as costs of online behavioural marketing is welcome. Typical measures such as click-through rates, average frequency of exposures, frequency to conversion ratio, ad exposure time (rich media), interaction rate (rich media) and web page eye tracking ultimately fail to capture neither the bottom line impact of additional sales, nor revenue lost through consumer disenfranchisement.

Finally, the variety and functions of advertising intermediaries lying between marketers and consumers are currently shrouded in mystery. Further empirical research describing and analysing the relationships between various intermediary players would significantly enhance understanding and refine the privacy debate.

Conclusion

A range of radically new marketing models are emerging, which bring a host of privacy issues sharply into focus. The framework of the current paper suggests that online privacy should be viewed as an exchange of consumers' personal information for online benefits (and annoyances). This means that one of the ways in which consumers are likely to evaluate an exchange of this sort is according to the principles of justice. Based on the organisational and social psychological literature, we have identified two classes of privacy concerns that consumers are likely to have: concerns relating to distributive justice and those relating to procedural justice. The former entail a judgment of the fairness of the distribution of consumers' and firms' outcomes relative to their inputs. The latter entails a judgment as to whether firms' actions violated important prescriptive norms. A justice framework suggests that consumers will also attend to the firm's outcomes (and both of their inputs) as well as the manner in which the information was collected. Justice theory predicts that these concerns will exert an independent influence on consumers' judgments of fairness, meaning that even fair payment for personal information can still lead to perceptions of unfairness if it is collected in a manner that violates a prescriptive norm (and vice versa). In turn, perceptions of unfairness are likely to lead to a variety of negative behaviours that firms' cannot afford to ignore.

Smith (1994) demonstrates how "drifting and reacting" is a common response of major North American companies to the privacy issue. That is, unless the organization is thrust into the public limelight in front-page articles or frenzied discussion on privacy newsgroups on the Internet, there is often little incentive to make privacy a priority. However, the present work suggests that firms need to be proactive in developing their privacy policies. Not only are consumers becoming increasingly aware of online privacy breaches but they are also better equipped to prevent privacy intrusions and retaliate against firms that are perceived to have acted inappropriately.

Notes

[1] The phrase "dataveillance" was first used by Clarke (1989) to describe the collection and storage of personal data enabled by computerization.

[2] Consumers appear to be less concerned about the collection and usage of information regarding their product purchases and media habits and more concerned about the collection and usage of medical records, social security numbers and financial information (Nowak and Phelps, 1992).

References

Acquisti, A. and J. Grossklags: 2005, 'Privacy and Rationality in Individual Decision Making', *IEEE Security and Privacy* **3**(1), 24–30.

Adams, J. S.: 1965, 'Inequity in Social Exchange', in L. Berkowitz (ed.), *Advances in Experimental Social Psychology* Vol. 2 (Academic Press, New York), pp. 267–299.

America Online and National Cyber Security Alliance: 2004, AOL/NCSA Safety Study, at http://www.staysafeonline.info/news/safety_study_v04.pdf.

Bagozzi, R.: 1975, 'Marketing as Exchange', *Journal of Marketing* **39**(4), 32–39.

Bennett, C. J.: 2004, 'Privacy Self-Regulation in a Global Economy: A Race to the Top, the Bottom or Somewhere Else?', in K. Webb (eds.), *Voluntary Codes: Private Governance, the Public Interest and Innovation*. (Carleton University, Ottawa), pp. 210–226.

Bentivoglio, J., N. Cortez and S. Kirk: 2003, 'Global Privacy Law Update', *The Computer and Internet Lawyer* **20**(6), 1–6.

Bies, R. J. and J. S. Moag: 1986, 'Interactional Justice: Communication Criteria of Fairness', in R. J. Lewicki, B. H. Sheppard and M. Bazerman (eds.), *Research on Negotiation in Organizations* Vol. 1 (JAI Press, Greenwich, CT), pp. 43–55.

Brockner, J. and B. Wiesenfeld: 1996, 'An Integrative Framework for Explaining Reactions to Decisions: Interactive Effects of Outcomes and Procedures', *Psychological Bulletin* **120**(2), 189–208.

Caudill, E. M. and P. E. Murphy: 2000, 'Consumer Online Privacy: Legal and Ethical Issues', *Journal of Public Policy and Marketing* **19**(1), 7–19.

Cespedes, F. V. and J. H. Smith: 1993, 'Database Marketing: New Rules for Policy and Practice', *Sloan Management Review* **34**(4), 7–23.

Chen, K. and A. I. Rea: 2004, 'Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques', *Journal of Computer Information Systems* **44**(4), 85–92.

Cialdini, R. and M. Trost: 1998, 'Social Influence: Social Norms, Conformity and Compliance', in D. Gilbert, S. Fiske and G. Lindzey (eds.), *The Handbook of Social Psychology*4th edition, Vol. 2 (Oxford University Press, New York), pp. 151–192.

Clarke, R.: 1989, 'Information, Technology, and Dataveillance', *Communications of ACM* **31**(5), 498–512.

Colquitt, J., D. Conlon, M. Wesson, C. Porter and K. Yee Ng: 2001, 'Justice at the Millenium: A Meta-Analytic Review of 25 Years of organisational Justice Research', *Journal of Applied Psychology* **86**(3), 425–445.

Cropanzano, R. and M. Ambrose: 2001, 'Procedural and Distributive Justice Are More Similar than You Think: A Monistic Perspective and a Research Agenda', in J. Greenberg and R. Cropanzano (eds.), *Advances in organisational Justice*. (Stanford University Press, Stanford, CA), pp. 119–151.

Deutsch, M.: 1985, *Distributive Justice* (Yale University Press, New York).

Falk, A., E. Fehr and U. Fischbacher: 2005, 'Driving Forces Behind Informal Sanctions', *Econometrica* **73**(6), 2017–2030.

Folger, R. and M. Konovsky: 1989, 'Effects of Procedural and Distributive Justice on Reactions to Pay Raise Decisions', *Academy of Management Journal* **32**(1), 115–130.

Foxman, E. and P. Kilcoyne: 1993, 'Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues', *Journal of Public Policy and Marketing* **12**(1), 106–19.

Greenberg, J.: 1993, 'The Social Side of Fairness: Interpersonal and Informational Classes of Organizational Justice', in R. Cropanzano (eds.), *Justice in the Workplace: Approaching Fairness in Human Resource Management*. (Lawrence Erlbaum Associates, Hillsdale, NJ), pp. 79–103.

Hetcher, S.: 2001, 'Norm Proselytizers Create a Privacy Entitlement in Cyberspace', *Berkeley Technology Law Journal* **16**, 877–935.

Homans, G. C.: 1961, *Social Behavior: Its Elementary Forms* (Routledge and Kegan Paul, London).

Kahneman, D. and A. Tversky: 1979, 'Prospect Theory: An Analysis of Decision under Risk', *Econometrica* **47**(2), 263–291.

Kotzer, J. A.: 2003, 'The Great Cookie Caper: Internet Privacy and Target Marketing at Home and Abroad', *St Thomas Law Review* **15**, 727–756.

Kulik, C. T. and M. L. Ambrose: 1992, 'Personal and Situational Determinants of Referent Choice', *Academy of Management Review* **17**(2), 212–237.

Leventhal, G. S.: 1980, 'What Should Be Done with Equity Theory? New Approaches to the Study of Fairness in Social Relationships', in M. Greenberg and R. Willis (eds.), *Social Exchange: Advances in Theory and Research*. (Plenum, New York), pp. 27–55.

Lind, E. and T. Tyler: 1988, *The Social Psychology of Procedural Justice* (Plenum, New York).

Miller, D. T.: 2001, 'Disrespect and the Experience of Injustice', *Annual Review of Psychology* **52**, 527–553.

Miller, S. and J. Weckert: 2000, 'Privacy, the Workplace, and the Internet', *Journal of Business Ethics* **28**(3), 255–265.

Milne, G. R. and M. E. Gordon: 1993, 'Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract', *Journal of Public Policy and Marketing* **12**(2), 206–215.

Milne, G. R., A. J. Rohm and S. Bahl: 2004, 'Consumers' Protection of Online Privacy and Identity', *Journal of Consumer Affairs* **38**(2), 217–232.

Nowak, G. J. and J. Phelps: 1992, 'Understanding Privacy Concerns: An Assessment of Consumers' Information

Related Knowledge and Beliefs', *Journal of Direct Marketing* **6**(4), 28–39.

Nowak, G. J. and J. Phelps: 1995, 'Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When 'Privacy' Matters', *Journal of Direct Marketing* **9**(3), 46–60.

OECD: 2003, Privacy Online: OECD Guidance on Policy and Practice, at http://www.1.oecd.org/publications/e-book/9303051E.PDF.

Palmer, D.: 2005, 'Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices', *Journal of Business Ethics* **58**(1), 271–280.

Petrison, L. A. and P. Wang: 1993, 'Exploring the Dimensions of Consumer Privacy: An Analysis of Coverage in British and American Media', *Journal of Direct Marketing* **9**(4), 19–37.

Pew Research Center: 2000, Trust and Privacy Online: Why Americans Want to Rewrite the Rules, at http://www.pewinternet.org/reports/toc.asp?Report=19.

Ranganathan, C. and S. Ganapathy: 2002, 'Key Dimensions of Business-to-Consumer Websites', *Information and Management* **39**(6), 457–465.

Rogers, J. L.: 1996, 'Mail Advertising and Consumer Behaviour', *Psychology and Marketing* **13**(2), 211–233.

Sarathy, R. and C. Robertson: 2003, 'Strategic and Ethical Considerations in Managing Digital Privacy', *Journal of Business Ethics* **46**(2), 111–126.

Sheehan, K. and M. Hoy: 2000, 'Dimensions of Privacy Concern among Online Consumers', *Journal of Public Policy and Marketing* **19**(1), 62–73.

Smith, H. J.: 1994, *Managing Privacy: Information Technology and Corporate America* (University of North Carolina Press, Chapel Hill, NC)

Taylor, C. R.: 2004, 'Consumer Privacy and the Market for Customer Information', *The Rand Journal of Economics* **35**(4), 631–650.

Thaler, R.: 1985, 'Mental Accounting and Consumer Choice', *Marketing Science* **4**(3), 199–214.

Thibaut, J. W. and L. Walker: 1975, *Procedural Justice: A Psychological Perspective* (Lawrence Erlbaum Associates, Hillsdale, NJ).

Trurow, J.: 2004, Americans and Online Privacy: The System is Broken, A Report from the Annenberg Public Policy Center of the University of Pennsylvania.

Tyler, T. R. and E. A. Lind: 1992, 'A Relational Model of Authority in Groups', in M. P. Zanna (eds.), *Advances in Experimental Social Psychology* Volume 25 (Academic Press, San Diego, CA), pp. 115–191.

Vermunt, R., D. van Knippenberg, B. van Knippenberg and E. Blaauw: 2001, 'Self-Esteem and Outcome Fairness: Differential Importance of Procedural and Outcome Considerations', *Journal of Applied Psychology* **86**(4), 621–628.

Walster, E., E. Berscheid and W. Walster: 1973, 'New Directions in Equity Research', *Journal of Personality and Social Psychology* **25**(2), 151–176.

Laurence Ashworth
Queen's School of Business,
Queen's University,
143 Union Street, Kingston,
Ontario, K7L 3N6,
Canada
E-mail: lashworth@business.queensu.ca

Clinton Free
Queen's School of Business,
Queen's University,
143 Union Street, Kingston,
Ontario, K7L 3N6,
Canada
E-mail: cfree@business.queensu.ca

Testimony on Alaska SB 118

Matthew Erickson
Digital Privacy Alliance

April 3, 2018

Chairperson, members of the committee, thank you for the opportunity to testify on SB 118, the "Right to Know Act". I am the executive director of the Digital Privacy Alliance, a nonprofit made up of tech companies, technologists, attorneys, academics, and common citizens that recognize a need for better consumer privacy online. I am also the Director of Client Services and Technology for SpiderOak, a technology company dedicated to online privacy and security. This bill is essential in guarding Alaskan citizens' privacy and seeks to give Alaskans the information they need to be able to make informed market choices about with whom they share their personal data with by ensuring that once every twelve months Alaskans can request a report from online services as to what data of theirs was shared with whom. I am particularly glad to be testifying in Alaska, as Alaska has shown itself as a leader in protecting personal information rights. I'd like to start by discussing the problems that we need to overcome.

Today's world all but requires people to be interacting through the Internet to accomplish everyday tasks, from banking and healthcare, to purchasing goods and services, and to connecting with friends and family. My attendance here providing testimony is based on outreach made over the Internet. This greatly empowers people all over the globe, especially those formerly isolated, making commerce stretch farther and the world seem smaller. Unfortunately, much of our activity in this new everyday life is recorded, collected, and sold to unknown places for unknown purposes. This unregulated data collection has stark consequences in light of not just the increasingly-common data breaches, but the revelations of the collaboration between Facebook and Cambridge Analytica. It is important that

we as a society empower everyday people to know what is going on with the data that represents who they are.

In today's age, corporations are collecting data on people all across the Internet via a wide variety of means to monetize that data and better market to those people. In a broad view, that's not the problem. Marketing-based systems have created a means to monetize increasingly better online tools that have enabled more and more people to be able to afford higher quality tools to communicate around the world. Unfortunately, that data is often abused, breached, or otherwise misused in ways that go far beyond funding development of a platform. Facebook, Twitter, and Instagram provided warrantless live streams of protest data to law enforcement through a company called Geofeedia in 2016[1]. Regular massive data breaches illustrate just what dangers we face from the large centralized collection of personal information. Alaskans suffer through having their personal information revealed by organizations they may have no knowledge of even interacting with.

Normally, we would first hope that if a company is a bad actor, people would cease doing business with it and it will naturally either correct its actions or go out of business. This is why we put value in organizations such as the Better Business Bureau. However, we lack the information to make such choices in the online space. Organizations such as Facebook will commonly track users not just outside of the Facebook website, but also people who have chosen to not have a Facebook account to begin with[2]. How are we, as individuals, supposed to make decisions on who gets the business of our personal data online without appropriate knowledge to support these decisions? No other industry gets to effectively charge you what they want for service and hide the invoice. And unlike other forms of payment, your personal information can't be gotten back once it's shared.

Arguments against providing these invoices to customers typically take the form that they are undue burdens on businesses. However, businesses will be able to comply easily with a minimum of overhead. Generally speaking, there are two broad categories of how organizations collect and sell data: either they handle it simply, where all user data in given categories is collected and set to a set number of advertising partners, or they have more complicated schemes. In the first case, a form letter is generally all that will be necessary. At the simplest end, an auto-responder can issue reports on demand. More complex uses of user data will be

[1]https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter

[2]https://spideroak.com/articles/facebook-shadow-profiles-a-profile-of-you-that-you-never-created/

necessarily accounted for already within company databases. When a company is built on monetizing user data in this manner, it will have an understanding of what was sold to whom and for how much, this being a necessity to properly provide fiscal accounting for the business. Reports can then be generated for users under the terms of this bill out of this same data. Additionally, larger multinational companies, or any company wishing to extend overseas, already has to comply with similar regulations in the EU and Canada, making compliance a simple matter of enabling the same functionality for Alaskans.

Finally, many organizations are now seeing trends towards growing distrust in the online economy. A recent Guardian headline asked if 2018 was the "year of the neo-Luddite?"[3]. Small startups labor most not under regulatory burden, but the problems of trying grow revenue. A growing distrust of online services only serves to slow down business. If the legislature wishes to help small businesses grow, the best thing it can do is help level the playing field for consumers to regain that trust.

Technological innovation is incredibly useful and beneficial to society. It saves time and money, and can also save lives. Analytics-driven service monetization also makes the cost of many advanced services down to what people have to spend-which for poorer citizens, is their personal information. It's not complicated for business to make sure citizens are empowered to choose with whom they share their personal data, and in return they can reverse the trend of increasing distrust in participating in the online economy. This bill will help make sure that the citizens of Alaska can have that trust. Thank you.

[3]https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite

STATE PRIVACY AND SECURITY COALITION

April 3, 2018

Chairman Kevin Meyer
Senate State Affairs Committee
State Capitol Room 103
Juneau AK, 99801

Re: AK SB 118, the "Right to Know" Act

Dear Chairman Meyer and Members of the Committee,

The State Privacy and Security Coalition, a coalition of 23 leading communications, technology, retail, and media companies and six trade associations, opposes Alaska SB 118, the Right-to-Know Act. For the reasons discussed herein, the bill would actually be detrimental to consumers and would create a very costly compliance burden for businesses, thereby discouraging investment in the State. It would create a strong incentive for companies to make all data that they disclose individually identifiable in order to be able comply with the law (a move that could harm consumers rather than helping them), and would impose needless legal expense with minimal public benefit. Finally, the bill is unnecessary – nearly every business with a website voluntarily discloses what types of information it collects and how it shares that information in its online privacy policy.

It is important to understand that that the Right-to-Know Act would be a total outlier with requirements that go far beyond any federal or state law, and would actually make consumers more identifiable, because the bill requires companies to not only begin keeping consumer information in a form that will be linkable and identifiable, but to sort through current customer information and make it identifiable. This requirement is not an incidental part the bill – requiring accountings of information that is not identified is the bill's central tenet. It would undermine consumer privacy by creating strong disincentives against companies for taking the pro-privacy step of keeping data in a form that very likely does not identify individuals, but might theoretically be "capable of" re-identification.

Moreover, businesses (even many small businesses) in the state would have to hire lawyers to decipher its complex requirements and then spend huge sums of money tracing disclosures of information that may not actually identify an individual.

It would also divert significant IT resources away from initiatives that advance innovation or cybersecurity, instead putting those resources towards extensive legal and technical compliance measures to avoid enforcement risk.

Under California's much more workable "Shine the Light" law (Cal. Civ. Code § 1798.83), which has been in operation for more than 15 years, our members have established compliance

systems but typically receive only a handful of legitimate requests each year regarding disclosures of personally identifying information to third parties for marketing purposes. Many of the requests received are actually fraudulent requests for information, including spam, fraud, or phishing attempts. Because of enforcement risk under the bill, businesses would be forced to address all of the fraudulent requests, which requires re-identifying de-identified data in an attempt to confirm that the people making the requests are who they say they are.

Although the bill says that it applies to the defined term "customers," nowhere does this legislation limit its reach to Alaskan residents, encompassing anyone who uses the internet who provides a sweeping range of non-personally identifying information to a business. This means the bill would reach every website or other service to which a person connects with a device, whether for business purposes or as a consumer. In many cases, businesses will not even have name and address information for these "customers" to be able to authenticate them and tie them to disclosures, but must somehow furnish an accounting of all businesses that received non-identifiable or identifiable information about the "customer" from the business.

We further caution against attempting to mandate particular forms of notice or to require placing privacy disclosures and statements of consumers' rights in online terms of use (as this bill would require). Indeed, these kinds of laws and enforcement criteria effectively require businesses to provide lengthy disclosures - which consumers are less likely to read -- in order to avoid costly enforcement actions.

The private right of action contained in the bill compounds the problems the bill would create. The vague and far-ranging requirements of this bill mean that a business could, for example, be found in violation of the statute if it failed to disclose that it had shared how many of its uses have college degrees with a marketer, while knowing no other information about the individuals. This is an invitation to an explosion of class-action litigation that will make lawyers happy and consumers less safe. Again, the bill's insistence on requiring shared data to be identifiable puts all Alaskan residents at risk.

Increased consumer transparency can be achieved without legislative mandates such as these. Furthermore, important progress has already been made on consumer transparency through self-regulatory efforts, such as the National Telecommunications and Information Administration ("NTIA") multi-stakeholder process, which created an FTC-enforceable code of conduct on mobile application transparency for participating companies.

Our coalition members recognize that privacy is very important and vigilantly and proactively working to keep users, subscribers, and customers safe. While this bill does not accomplish that objective, we would be happy to discuss best practices for data security at your convenience.

For the foregoing reasons, we respectfully request that AK SB118 be withdrawn.

Sincerely,

Jim Halpert
Counsel, State Privacy & Security Coalition

April 3, 2018

Honorable Kevin Meyer
Senate State Affairs Committee, Chair
State Capitol Room 103
Juneau, AK 99801

Dear Chair Meyer:

The undersigned organizations write to respectfully **oppose SB 118**, which impedes the responsible collection and use of information that is vital to large and small businesses and is a crucial component of the Alaska economy. If enacted, SB 118 would turn Alaska into an outlier among the states, making Alaska a more difficult place to innovate on the Internet. Such a move would hurt the information economy that has become an important part of the Alaska economy.

The undersigned organizations oppose state legislation that needlessly places restrictions on the flow of data, or otherwise harms the information economy. SB 118 is such a bill. We oppose for the following reasons.

SB 118 is Unnecessary. The current protections in place for consumers on the Internet, via disclosure and choice, have worked. These practices have developed along with the Internet. They are flexible depending upon the type of consumer data, and have enabled innovation on the Internet to occur. The Internet is flourishing, and that is because people want to use it and are comfortable using it. SB 118 is a solution searching for a problem. It would add additional, needless steps that companies on the Internet will have to take, which will not help consumers.

SB 118 is Unworkable. SB 118 would place extraordinary reporting and tracking requirements on businesses operating on the Internet. The bill would require businesses to create a system that enables the business to provide a consumer with a report about nearly every piece of information that the consumer has provided to the business. Such a system would be very costly and would likely provide little benefit to consumers.

While SB 118 envisions exceptions to the reporting requirement and thus acknowledges that this information must be collected, used, and shared for the Internet to function, such exceptions will not protect businesses from having to take extraordinary measures to ensure they comply with the law. The resources for tracking and reporting will be expended whether or not a reporting requirement exists.

As discussed further below, the private right of action in SB 118 will force businesses to contend with frivolous lawsuits, even when they are in compliance. As these cases are brought, millions of dollars in litigation will be spent before a judge ever considers whether a company was in compliance because of an exception to the reporting requirement.

SB 118 conflicts with other laws. SB 118 creates compliance requirements that diverge from current law in other states. Inconsistent state laws make it more difficult for businesses to offer services on the Internet to consumers across the country. Such a "patchwork" of state laws can be incredibly damaging, and can slow down the growth of the Internet, along with the innovative services that are being developed. SB 118 will have the opposite result of its desired effect. SB 118 and bills like it harm consumers more than they help because they do not provide protections to consumers that are needed, and they make it more difficult for consumers to receive the services that they clearly want.

The Proposed Definition of "Personal Information" is Overly Broad. The proposed definition of "personal information" would impose requirements on data beyond that which is used to identify an individual. This proposed definition is well outside the bounds of what other states and the federal government have designated as "personal information" under the law. The bill defines "personal information" as anything 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, physical characteristics or description, address, telephone number, passport number, driver's license or state identification number..." These data elements alone do not identify an individual.

Federal Trade Commission Staff has rejected a similar standard, stating that "the proposal to include any data that is 'linkable' [within the definition of personal information] could unnecessarily limit the use of data that does not pose a risk to consumers. While almost any piece of data could be linked to a consumer, it is appropriate to consider whether such a link is practical or likely in light of current technology."[1] The phrase "capable of being associated with" within SB 118 faces similar complications.

SB 118 would lead to frivolous lawsuits. SB 118 would provide plaintiffs' lawyers a means to bring frivolous lawsuits against companies operating on the Internet. Because consumers already have adequate protections in place, if enacted, SB 118 would merely increase the cost of doing business in Alaska, without providing actual benefits to consumers. Alaska is attempting to position itself as a center for innovation and growth in the data economy. The private right of action provision in SB 118 would do the opposite.

Self-Regulation has been effective. Further, enacting SB 118 to protect consumers is unnecessary because data-driven marketing is already effectively governed by strong and enforceable self-regulatory codes. Industry self-regulation can adapt rapidly to new technologies and marketing practices, as opposed to legislative solutions that often prove to be too inflexible to quickly respond to the rapidly-developing technological environment.

---

[1] Federal Trade Commission Bureau of Consumer Protection Staff, Comments on Notice of Proposed Rulemaking, FCC WC Docket No. 16-106, at 9 (May 27, 2016).

One example of these industry self-regulatory practices is the establishment of individual company privacy policies. These privacy policies typically provide consumers with information regarding what types of data are collected, how it is used and the options that may be available to consumers to opt out of such data collection activities. Current industry standards also require that providers must, when requested by a consumer, discontinue the use of and suppress that consumer's data in marketing databases. Legislative action is unnecessary as existing industry standards already provide consumers with transparency about how their personal information is being collected and how it is used.

Because it unduly burdens Alaska's small businesses and nonprofits, negatively impacts Alaska's data-driven economy and jobs, and is unnecessary, the undersigned organizations respectfully **oppose SB 118**.

Sincerely,

Data & Marketing Association
ANA – Association of National Advertisers
CompTIA – Computing Technology Industry Association
Internet Association
Internet Coalition
MPA – The Association of Magazine Media
NetChoice
Network Advertising Initiative
TechNet

cc: Members of the Senate State Affairs Committee

Fiscal Note

State of Alaska
2018 Legislative Session

Bill Version: SB 118
Fiscal Note Number:
() Publish Date:

Identifier: SB118-LAW-CIV-03-30-18
Title: DISCLOSURE OF CUSTOMER INFORMATION
Sponsor: WIELECHOWSKI
Requester: Senate State Affairs

Department: Department of Law
Appropriation: Civil Division
Allocation: Commercial and Fair Business
OMB Component Number: 2717

Expenditures/Revenues

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2019 Appropriation Requested	Included in Governor's FY2019 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY 2019**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**	**FY 2024**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
Total Operating	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Fund Source (Operating Only)

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Positions

Full-time							
Part-time							
Temporary							

Change in Revenues

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimated SUPPLEMENTAL (FY2018) cost: 0.0 *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY2019) cost: 0.0 *(separate capital appropriation required)*
(discuss reasons and fund source(s) in analysis section)

ASSOCIATED REGULATIONS

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? No
If yes, by what date are the regulations to be adopted, amended or repealed?

Why this fiscal note differs from previous version/comments:

Not applicable, initial version.

Prepared By: Valerie Rose, Budget Analyst — Phone: (907)465-3674
Division: Administrative Services Division — Date: 03/30/2018 01:00 PM
Approved By: Jahna Lindemuth, Attorney General — Date: 03/30/18
Agency: Department of Law

FISCAL NOTE ANALYSIS

STATE OF ALASKA
2017 LEGISLATIVE SESSION

BILL NO. SB 118

Analysis

SB 118 adds new sections to the Personal Information Privacy Act (AS 45.48) to protect disclosure of personal information and provide transparency when information is sold or disclosed. The bill provides that the owner of an internet website or commercial online service ("owner") must (1) identify categories of personal information collected about customers, (2) identify third parties to whom the owner discloses (or may disclose) the personal information, (3) describe a customer's rights (as set out in newly-created AS 45.48.810), and (4) provide an address, email or phone number that the customer may use to request or obtain information the owner is required to provide.

An owner that discloses a customer's personal information to a third party must, without charge, tell the customer of the disclosure within 30 days of a request, and must include the categories of personal information disclosed, and the names of third parties that received the information.

The bill outlines twenty categories of personal information implicated by its requirements and provides for three exemptions from the disclosure requirements: (1) when contractually exempt, (2) when the owner is complying with a legal process or court order, and (3) when necessary to address fraud or technical issues. The bill does not apply to governmental agencies or its contractors, subcontractors, or agents. A customer whose information was subject to a violation would be able to maintain an action to recover money damages or other relief.

The Department of Law is uncertain of the number of potential actions that may arise if the bill becomes law, but since the bill provides a private cause of action, the Department of Law expects no fiscal impact if this bill should become law.