IMPROVING DATA SECURITY IN ILLINOIS:

PROPOSED UPDATES TO THE PERSONAL INFORMATION PROTECTION ACT

DISCLOSURE

PROTECTION

NOTIFICATION

LISA MADIGAN
ILLINOIS ATTORNEY GENERAL

Table of Contents

IMPROVING DATA SECURITY IN ILLINOIS:
PROPOSED UPDATES TO THE PERSONAL INFORMATION PROTECTION ACT

Executive Summary

This year, the Illinois Attorney General's office is seeking to update the Illinois Personal Information Protection Act (PIPA) in an effort to better protect the sensitive, personal data of Illinois residents. Illinois first passed PIPA in 2005 to ensure consumers were notified of breaches related to their social security numbers, drivers' license numbers, or financial account information. Nearly a decade later, this law is out-of-date.

In the ten years since Illinois first passed the law, the type of information that can harm consumers, if used improperly, has greatly expanded and the frequency of data breaches has greatly increased. In responding to these challenges since 2005, the Illinois Attorney General's office has:

- investigated the circumstances leading to dozens of data breaches;
- reviewed privacy policies and requested information from entities to better understand the nature of the consumer data being collected;
- convened consumer roundtables; and
- helped thousands of Illinois residents respond to identity theft.

This work has informed the office about the current data security challenges facing consumers and entities that collect data. These challenges include:

Entities are failing to take basic steps to secure sensitive consumer data. The investigations into data breaches that the Illinois Attorney General's office has conducted show that many data breaches are the result of entities failing to take basic steps to protect data.

PIPA does not cover a significant percentage of the sensitive consumer data that entities collect and store. In the past decade, the Internet has become much more integrated into the daily lives of consumers and, as a result, increasingly specific, personal information about consumers is now being collected and stored. But this information, for the most part, is not covered by PIPA. For example, a breach of consumers' login credentials (usernames and passwords) for online accounts is not addressed in Illinois law.

Data breaches can cause reputational harm, as well as financial harm. Data breach statutes have focused on the financial impacts of data breaches. However, with the expansion of data collection, this sensitive information now includes information, like geolocation information, that can also lead to "reputational harm."

Data breach notification to consumers can be improved. During roundtables on data security that the Attorney General's office convened over the past year, consumers regularly informed staff that, while they were aware that data breaches were occurring, they were not aware when those breaches affected them specifically.

Consumers are not always notified when their sensitive information is collected, stored, or shared. Many websites and apps are now collecting, storing, and sharing sensitive data about consumers, and consumers are not always notified or aware that this is occurring.

To address these challenges, the Illinois Attorney General's office is proposing the following updates to PIPA. The proposed updates to PIPA are included with one of the three principles that they serve:

Principle One: Disclosure ***If an entity collects sensitive information about a consumer, the entity should disclose that to the consumer.***

- **Proposal:** Require websites and apps that collect personal information to display privacy policies that explain what information is collected and who that information is shared with.

Principle Two: Protection ***If an entity collects sensitive information about a consumer, the entity should take reasonable steps to protect the information.***

- **Proposal:** Require entities to establish reasonable security measures to safeguard sensitive personal information.

Principle Three: Notification ***If an entity fails to protect that sensitive information, the public should be notified of the breach.***

- **Proposal:** Expand the definition of personal information to include medical information, health insurance information, biometric data, geolocation information, sensitive consumer marketing data, contact information when combined with additional identifying information like date of birth, and login credentials for online accounts.
- **Proposal:** Require entities to notify the Illinois Attorney General's office when breaches occur so the office can create a website for Illinois residents, which lists the data breaches that have affected Illinois.
- **Proposal:** Enable small businesses to notify local media, rather than statewide media, when breaches occur.

I. Introduction

This report provides: (1) an overview of the Illinois Attorney General office's work on identity theft and data security; (2) the data security challenges currently facing Illinois residents; and (3) the office's legislative recommendations for addressing those challenges. The solutions proposed in this report have been placed within the bill (SB 1833) that Senator Biss introduced. While these proposals cannot eliminate data breaches or identity theft, they can help improve data security and ensure transparency when breaches do occur. Security experts agree that entities can take better data security steps to protect data, and additional transparency surrounding the breaches that do occur will only help ensure entities that collect data take better steps to protect it.

Government agencies, at both the state level and the federal level, must continue to play an important role ensuring that entities take the proper steps to protect consumer data, and notify consumers when their sensitive information is compromised. To address our country's security vulnerabilities, the government, the private sector, non-profits, and consumers must work together. The challenge cannot be met without cooperation at all levels. This report summarizes the Illinois Attorney General's office current strategy for addressing this challenge, as well as the information that led to the development of the strategy.

The work of the Attorney General's office in recent years has led the office to conclude that Illinois law must be updated to keep pace with the growth in data collection and the increased threat of cyber attacks. This report explains that conclusion. It is a product of the investigations the office has conducted, staff research into the current data security and data collection practices in the private sector, and consumer roundtables that the office has convened.

II. Background

a. The Role of the Illinois Attorney General's Office in Data Security and Identity Theft

The Illinois Attorney General's Office has been investigating data breaches and responding to identity theft for over a decade. This authority stems from two Illinois statutes and one federal statute. Under the Illinois Consumer Fraud and Deceptive Business Practices Act, the Attorney General's office has general authority to investigate "unfair and deceptive practices."[1] As discussed below, the office uses this authority to investigate the data security practices of entities that suffered data breaches to ensure the entities were using reasonable data security practices to protect the breached information. The Federal Trade Commission uses similar authority to conduct investigations at the federal level.

In 2005, at Attorney General Madigan's direction, Illinois passed the Personal Information Protection Act (PIPA).[2] Illinois was among the first states in the country to enact such legislation. To help consumers take steps to prevent identity theft, PIPA requires entities that suffer a data breach to notify Illinois residents if the breached information included

[1] 815 ILCS 505.

[2] 815 ILCS 530/1 (e.t. seq.), Ill. Public Act 94-36 (2005).

residents' drivers' license numbers, Social Security numbers, or financial account information.[3] In 2011, PIPA was updated to include a requirement that entities with sensitive data take steps to properly dispose of that data.[4]

In 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which requires entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to report data breaches of health information to the affected individuals. Congress gave the state attorneys general the authority to enforce this law, along with the Department of Health and Human Services.

The Illinois Attorney General's office also assists Illinois residents when they face identity theft. In 2006, Attorney General Madigan established an Identity Theft Unit and Hotline to provide information to consumers on how to prevent and respond to identity theft. Since 2006, the office has helped remove more than $27 million in fraudulent charges for more than 37,000 Illinois residents.

Using its authority under the Consumer Fraud and Deceptive Business Practices Act and the Personal Information Protection Act, the office has opened dozens of investigations into the data security practices of companies that have suffered data breaches, entities that have violated the privacy of its customers, and entities that improperly disposed of consumers' personal information. Significant settlements have occurred with the following companies:

- Choice Point for its sale of 145,000 consumer credit files to identity thieves;[5]
- TJX Companies for two breaches of credit card information, social security numbers, and other personal information affecting thousands of customers.[6]
- The Payday Loan Store of Illinois for allegations that it improperly disposed of nonpublic personal information by dumping unredacted paperwork in a dumpster behind the store.[7]
- Google Inc. and PointRoll, Inc. for allegations that companies unlawfully circumvented consumers' privacy settings on their Internet browsers. [8]

[3] Specifically, the law requires notification only when such information is attached to an individual's first name and last name, or initial and last name.

[4] 815 ILCS 530/40.

[5] Press Release, Illinois Attorney General Lisa Madigan, "Attorney General Madigan Reaches Agreement with ChoicePoint," May 31, 2007.

[6] Press Release, Illinois Attorney General Lisa Madigan, "Madigan, TJ Maxx Reach Agreement to Ensure Protection of Personal Data Following Massive Security Breach," June 23, 2009.

[7] Press Release, Illinois Attorney General Lisa Madigan, "Attorney General Madigan Sues Payday Loan Store After Customers' Personal Information Ends Up in the Trash," Oct. 15, 2010.

[8] Press Releases, "Madigan Announces $17 Million Settlement with Google," Nov. 18, 2013; "Madigan Announces Settlement Over Allegations That Digital Advertising Firm Breached Internet Privacy," Dec. 11, 2014.

- Watershed Development Corporation for allegations that the company used computer software to spy on consumers who rented laptops from their stores.[9]

The office also chairs the Privacy Working Group of state attorneys general through the National Association of Attorneys General (NAAG), which helps coordinate the efforts of the states when responding to national data breaches.

b. Recent Efforts by the Illinois Attorney General's Office

In recent years, due to the increasing number of significant data breaches, the Illinois Attorney General's office has opened a number of investigations into data breaches that have affected Illinois residents. Many of these investigations are ongoing. The office has also taken a number of steps to better understand the data security and privacy challenges facing consumers and to share the knowledge the office has gained in its investigations.

In 2013, Attorney General Madigan sent inquiry letters to eight health-related websites, requesting information about how they collect, store, and disclose consumer health information to better understand how companies treat this type of sensitive information.[10] As described below, the responses the office received in response to these requests has helped inform the legislation.

In 2014, the Attorney General held over 25 roundtables throughout Illinois. Nearly 1,000 residents from around the state attended – law enforcement officials, small business owners, consumers, and senior citizens. The office provided guidance on data security and identity theft, and the attendees shared valuable feedback with the office.

Finally, because of her expertise in data security and identity theft, Attorney General Madigan has been asked to testify on data security in Congress twice over the past year. In February 2014, she testified before the Subcommittee on Commerce, Manufacturing, and Trade in the U.S. House of Representatives. In February 2015, she testified before the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security in the U.S. Senate.

III. Current State of Data Security and Privacy

a. The Rise and Impact of Data Breaches

A data breach is the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. The data breaches that are most often reported in the media are those where a hacker infiltrates a company's servers and accesses sensitive information about the company or its customers. Data breaches also occur as a result of human or technical error.

[9] Press Release, "Madigan, FTC Crack Down on Rental Stores Spying on Consumers Via Rented Laptops," Sept. 25, 2012.

[10] Press Release, "Madigan: Popular Health Websites Must Ensure Privacy of Users' Health Information," July 12, 2013.

Data breaches have become regular occurrences. In 2014, more than 67 million records were involved in a data breach, and since 2005, more than 800 million consumer records have been compromised.[11] Most of the media attention has focused on large breaches that impact thousands or millions of consumers, but breaches can involve any size company, including small businesses.[12] In one survey, forty-four percent of small business owners reported that their company had been the victim of a cyber attack.[13] In 2013, at least 5,819 small businesses – organizations with fewer than 1,000 employees – suffered a security incident.[14]

Breaches also affect a range of organization types. While retailer breaches gained significant media attention recently due to their size, in 2013, consumer information was also compromised via credit card issuers, financial institutions, health care providers, gas stations, government agencies, universities, and others.[15]

Any type of information that a company holds can be involved in a data breach. Financial account information is the most targeted type of personal information, but breaches also result in the theft and misuse of Social Security numbers, names, physical addresses, usernames and passwords, drivers' license numbers, email accounts, health insurance information, and other forms of identification.[16] While the theft of credit card data can result in fraudulent charges, the theft of a Social Security number increases a consumer's risk of identity theft 18 times.[17]

Breaches are costly. One study claims that as many as one in three data breach victims can become victims of identity theft.[18] When an identity thief uses a Social Security number to take over a consumer's accounts, on average, it costs the consumer $5,100.[19]

The cost of securing a breach and protecting consumers from future harm can be considerable for entities suffering breaches as well. On average, a data breach costs companies

---

[11] Privacy Rights Clearinghouse, "Chronology of Data Breaches," accessed March 1, 2015, available at: https://www.privacyrights.org/data-breach.

[12] *See e.g.,* Los Angeles Times, "Small businesses at high risk for data breach," July 4, 2014; CNN, "Cybercrime's easiest prey: Small businesses," Apr. 23, 2013 ("Of the 621 confirmed data breach incidents…close to half occurred at companies with fewer than 1,000 employees, including 193 incidents at entities with fewer than 100 workers.").

[13] National Small Business Association, "2013 Small Business Technology Survey," Sept. 16, 2013, available at: http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf.

[14] Verizon Enterprise Solutions, "2014 Data Breach Investigations Report," p. 6, 2014.

[15] National Consumers League, "The Consumer Data Insecurity Report: Examining the Data Breach – Identity Fraud Paradigm in Four Major Metropolitan Areas," p. 15, June 2014.

[16] *Id. at 13.*

[17] *Id. at 14.*

[18] *Id. at 5.*

[19] Today, "Data breaches cost consumers billions of dollars," June 5, 2013, available at: http://www.today.com/money/data-breaches-cost-consumers-billions-dollars-6C10209538#.

$201 per compromised record.[20] Fifty-two percent of companies reported a loss in reputation or image following a breach,[21] the cost of which can amount to $3.2 million in lost business.[22]

b. Expansion of Data Collection

Data breaches are becoming both more common and more concerning because entities are storing increasingly specific data about consumers on servers connected to networks. This data goes beyond financial information, and it can include categories such as geolocation information, medical information, and online activity. As consumers continue to adopt mobile technology and use the Internet in their daily lives, their digital footprint will grow increasingly specific and, if misused, increasingly damaging.

1. Geolocation Information

Geolocation information captures an individual's movements in the physical world. It is collected by websites and mobile applications for a variety of reasons.[23] Mobile apps use geolocation information to help consumers find nearby restaurants, log their jogging routes, and get accurate weather forecasts. Companies also use geolocation to more accurately target their advertising and more effectively deliver their services.

This collection is not without risk, however. As noted by the Federal Trade Commission, "Geolocation information can divulge intimately personal details about an individual. Did you visit an AIDS clinic last Tuesday? What place of worship do you attend? Were you at a psychiatrist's office last week? Did you meet with a prospective business customer?"[24] Geolocation information can expose the private details of a person's life. Placed in the wrong hands, geolocation information can also raise very serious concerns about stalking and harassment.[25]

---

[20] Ponemon Institute Research Report and IBM, "2014 Cost of Data Breach Study: United States," p. 2, May 2014.

[21] Ponemon Institute Research Report and Identity Finder, "2014: A Year of Mega Breaches," p. 8, Jan. 2015.

[22] Ponemon Institute Research Report and IBM, "2014 Cost of Data Breach Study: United States," p. 2, May 2014.

[23] *See*, U.S. Government Accountability Office, "Mobile Device Location Data: Additional Federal Actions Could Help Protect Consumer Privacy," GAO-12-903, Sept. 2012; Ohm, Paul, "Sensitive Information," Southern Cal. Law Review, forthcoming Vol.88, available at: http://ssrn.com/abstract=2501002 (attributing the increase in collection of geolocation to prevalence of GPS chips in phones, availability of GPS information to smartphone app developers, and monetization of user location information by wireless providers).

[24] Prepared Statement of The Federal Trade Commission on S. 2171 The Location Privacy Protection Act of 2014, Before the United States Senate Committee on the Judiciary Subcommittee for Privacy, Technology and The Law (June 4, 2014), available at: http://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf.

[25] Ohm, Paul, "Sensitive Information," Southern Cal. Law Review, forthcoming Vol. 88, available at: http://ssrn.com/abstract=2501002.

2. Consumer Medical Information

U.S. privacy law recognizes that individuals have a privacy interest in their medical information. HIPAA requires health providers and insurers to secure consumers' medical information and to notify consumers in the event of a breach. Patients need such privacy to ensure that they can share and receive essential medical information without the fear of stigma or harassment.

With the growth of the Internet, consumers are now regularly sharing their medical information outside their doctors' offices and, as a result, outside the protections of HIPAA. For example, numerous mobile applications and websites are offering consumers services for tracking weight loss, monitoring glucose levels, researching medical conditions, and storing prescription information. A consumer sharing medical information with such websites or apps does not have the same privacy protections required by federal law in a doctor's office.

To better understand the practices of medical websites and apps, the office requested information from eight health-related privacy websites. The office's review of this information confirmed that consumer medical information is being collected and shared outside the scope of HIPAA. Companies generally provide heightened security and privacy protections to consumer medical information only when it is being stored in connection with a consumer's personally identifiable information (e.g. name, e-mail address, credit card number). Such protections may include encryption, access controls, and limits on sharing with third parties. But fewer protections are provided when consumers' medical information is revealed through search terms, page views, and health tools because companies typically do not consider this to be personally identifiable information. A recent study further confirmed the office's findings. The study found that, in a review of 80,000 health-related web pages, 70% of HTTP requests sent to third parties contained information about the page that the consumer was viewing, which could expose specific conditions, treatments, and diseases.[26]

3. Online Activity

When consumers use the Internet, websites and apps can collect information about which pages they visit, the search terms they enter, the information they share, the links that they click, and the products and services that they purchase. Over time, this online activity can reveal very specific details about the characteristics of one's life that could otherwise be considered personal and sensitive. For example, the FTC has acknowledged that collecting online search history information from consumers can be problematic, given that the collection "is typically invisible to consumers who may believe that they are searching anonymously for information about medications, disease, sexual orientation, or other highly sensitive topics."[27]

[26] Timothy Libert, "Privacy Implications of Health Information Seeking on the Web," Communications of the ACM, Vol. 58 No. 3, 68-77 (March 2015).

[27] Federal Trade Commission, "FTC Staff Report:Self-Regulatory Principles for Online Behavioral Advertising," Feb. 2009.

This proliferation of personal information has helped lead to the rise of data brokers – "companies that collect consumers' personal information and resell or share that information with others."[28] These companies collect consumer data from various sources, including browsing activity collected with cookies, and transaction history from retailers, financial service companies, and websites.[29] Data brokers typically do not collect this information directly from consumers, so consumers often are often unaware that sensitive information is being gathered about them.

The information collected by data brokers can be incredibly detailed. They can tell "whether consumers view a high volume of YouTube videos, the type of car they drive, ailments they may have such as depression or diabetes, whether they are a hunter, what types of pets they have, or whether they have purchased a particular shampoo product in the last six months."[30]

IV. Current Data Security Challenges

The rise in data breaches and the expanded collection of personal information have exposed the following vulnerabilities and weaknesses in our country's current data security regime:

- Personal information is not being adequately secured.
- Breach notifications are not as effective as they could be.
- Entities are not fully disclosing their data security and data privacy practices.

A. Data Security Can Be Improved

Although many entities do take data security seriously, the Attorney General's office has frequently seen a lack of basic best practices when investigating data breaches. The office's experiences match reports from data security experts. For example, in a review of data breaches that occurred in 2012, Verizon found that less than 1% of breaches were of high difficulty for initial compromise.[31] In 78% of breaches, the level of difficulty to initially gain access to the targeted database was low or very low. More recently, Symantec's Vice President of Global Government Affairs and Cybersecurity Policy testified in Congress that:

> Another major cause of breaches is a lack of basic computer hygiene practices. While good security will stop most of these attacks – which often seek to exploit older, known vulnerabilities – many organizations do not have up-to-date security or patched systems, do not make full use of the security tools available to them, or have security unevenly applied throughout their enterprise. Even today – despite the recent focus on the loss of

[28] Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability," May 2014.

[29] *Id.*

[30] UnitedStates Senate Committee on Commerce, Science, and Transportation, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes," ii, Dec. 28, 2013, available at: http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a.

[31] Verizon, "2013 Data Breach Investigations Report," p. 49.

personal information – a large segment of the workforce handles sensitive information on unprotected mobile devices, servers, desktops, and laptops.[32]

A common vulnerability exploited by hackers in the recent wave of data breaches is compromised login credentials stolen through targeted phishing[33] campaigns. In these cases, hackers target individuals via email to trick them into revealing their user credentials. Using these credentials, hackers then gain access to more sensitive information contained on the entity's servers. Seventy-six percent of network intrusions in 2012 exploited weak or stolen credentials.[34]

Since this tactic is so common, entities holding sensitive data should anticipate and respond to the threat of stolen credentials by using multi-factor authentication[35] to prevent access in the event that login credentials are stolen. The failure to use multi-factor authentication is just one example where companies are not following best practices. In the office's investigations of data breaches, the office has found instances where entities:

- allowed sensitive personal information to be stored unencrypted;
- failed to install security patches for known software vulnerabilities;
- collected sensitive information that the company did not need or use; and
- retained data longer than necessary.

Like multi-factor authentication, these steps are basic data security practices. Yet, entities suffering breaches were not taking them. Until these security vulnerabilities are addressed, data breaches of sensitive consumer information will continue.

B. Effectiveness of Breach Notification

The Illinois Personal Information Protection Act requires companies that collect information about Illinois residents to send breach notifications to consumers if there is a breach of consumers' first and last name, combined with their Social Security numbers, drivers' license numbers or financial account information.[36]

---

[32] McGuire, Cheri, "Testimony before the Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security," (Feb. 5, 2015), available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=00612a7f-39a3-4d7a-a16d-6042709e4c95.

[33] The Federal Trade Commission defines phishing as "when Internet fraudsters impersonate a business to trick you into giving out your personal information." Additional information can be found at: http://www.consumer.ftc.gov/articles/0003-phishing.

[34] Verizon, "2013 Data Breach Investigations Report," p. 6 (2013).

[35] Multi-factor authentication is a common data security practice that combines two or more independent credentials to prevent unauthorized access to systems and accounts. Examples of multi-factor authentication include two or more of the following categories: what the user knows (a password or security question); what the user has (a security token or ATM card); and what the user is (biometric information). Requiring more than one of these for login credentials makes it more difficult to provide false credentials.

[36] Illinois Personal Information Protection Act, 815 ILCS 530/.

Breach notifications enable consumers to proactively monitor their financial accounts and credit reports to ensure that they do not become victims of identity theft or financial fraud following a breach. After receiving a notification, consumers more closely monitor their accounts: 24% set up alerts on their credit or checking accounts and 23% place fraud alerts on their credit report.[37] These steps lower the risk of consumers becoming the victim of future fraud.

While breach notification has helped consumers take steps to protect themselves and increased the transparency of certain types of breaches, the breach notification requirements need to be updated to ensure their continued effectiveness. The Attorney General's office recent work responding to data breaches has exposed limitations in the law's effectiveness that can be addressed through legislation.

1. Limited Notification Triggers

Breaches can impact many types of information beyond those that currently trigger notification. Many types of sensitive information – medical information, geolocation information, biometric data, login credentials, search history – can be valuable to hackers and harmful to consumers if stolen.

For example, login credentials stolen in a breach from one company could provide access to many other accounts if the consumer has used those credentials at multiple websites. Those login credentials can be used repeatedly to access bank accounts, online shopping accounts or e-mail accounts.[38] Account credentials for iTunes, FedEx.com, Continential.com, United.com, Groupon.com and Facebook.com have been sold on the black market for anywhere between $2.50 and $8.00 per account.[39]

Other types of information, such as medical and geolocation information, create different risks. Medical information can be used to cause reputational embarrassment or facilitate medical fraud under the victim's name. Geolocation information could be sold for harassment or stalking purposes and could reveal sensitive details about a person's life.[40] Although this information is sensitive, consumers would not be notified of these breaches under current law.

[37] National Consumers League, "The Consumer Data Insecurity Report: Examining the Data Breach – Identity Fraud Paradigm in Major Metropolitan Areas," p. 17, June 2014.

[38] KrebsonSecurity.com, "The Value of a Hacked Email Account," June 10, 2013, available at: http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/.

[39] *Id.*

[40] Testimony of Mark L. Goldstein, Director, Physical Infrastructure Issues, U.S. Government Accountability Office, "Consumers' Location Data – Companies Take Steps to Protect Privacy, but Practices are Inconsistent, and Risks May Not be Clear to Consumers," GAO-14-649T, June 4, 2014.

2. Small Businesses May Find It Difficult To Comply And Notify Customers

Under PIPA, when breaches occur, entities must notify individuals.[41] Individualized notification may be excused if the entities do not have sufficient contact information for consumers, if the breach involves more than 500,000 individuals, or if individual notification would cost more than $250,000.[42] In those cases, companies can comply with the law by providing substitute notice, which consists of an email notice (if available), conspicuous posting to the company's website, and notification to statewide media.[43]

For large breaches, the exceptions to individual notice are designed to help ensure that affected consumers still receive notice. This is less effective for small, localized breaches. Contacting statewide media may be meaningless if that media coverage is not going to reach the part of the state where the affected consumers live. Furthermore, the media is unlikely to cover the story if it only has a small, local impact. The breach is no less significant, however, for those individuals whose information was stolen.

In those cases, small business need a way to ensure that their customers receive notification of the breach, without having to go through extra hoops that are not required for a large-scale breach. Localized notice is crucial to ensuring that consumers get the appropriate information.

3. Confusion Over Breaches

In 2014, the Attorney General held nearly 30 roundtables to discuss identity theft and data security with Illinois residents. The roundtables included local law enforcement, small business owners, senior citizens, and consumers. The most frequent complaint from participants was that they wanted more information about breaches that have occurred. Participants at the roundtables were well aware of the breaches that had been reported in the media, but they were not always aware if those breaches had affected them directly.

C. Data Collection Disclosure

Today, most websites have privacy policies. This is less true for mobile applications. And even if a company does have a privacy policy, it may not be particularly useful. Privacy policies are supposed to inform consumers about how a company collects, stores, and shares the information it collects about them. But that does not always occur, either because the policy is too vague or there is no privacy policy. For example, in a review of medical and health-related mobile apps, the Privacy Rights Clearinghouse found that 26% of free apps and 40% of paid apps did not have a privacy policy.[44]

---

[41] 815 ILCS 530/10(a).

[42] 815 ILCS 530/10(c).

[43] 815 ILCS 530/10(c).

[44] Privacy Rights Clearinghouse, "Mobile Health and Fitness Applications and Information Privacy – Report to California Consumer Protection Foundation," p. 5, July 15, 2013.

V. Proposals to Address Data Security Challenges

To address the challenges facing consumers and data collectors, the Attorney General's office is proposing amending the Illinois Personal Information Protection Act. The proposed updates to the Personal Information Protection Act serve one of three basic principles:

- **Principle One:** If an entity collects sensitive information about a consumer, the entity should disclose that to the consumer.

- **Principle Two:** If an entity collects sensitive information about a consumer, the entity should take reasonable steps to protect the information.

- **Principle Three:** If an entity fails to protect that sensitive information, the public should be notified of the breach.

These principles help explain what the Illinois Attorney General's office intends to accomplish with the proposed updates to PIPA. The specific proposals that help achieve each principle are discussed below.

A. Disclosure to Consumers

Proposal: Require websites and apps that collect personal information to display privacy policies that explain what information is collected and who that information is shared with.

In 2003, California passed a law requiring entities to post privacy policies on their websites or online services, if the website or online service collects personally identifiable information about consumers. The law requires companies to disclose their data collection activities to consumers, and a recent amendment requires them to disclose how they respond to "Do Not Track" signals.

The Illinois Attorney General's office recommends passing similar legislation so that our state has the same enforcement options as California. Further, with the sensitive information that companies can now collect about consumers via their online activity, the office believes it is imperative that companies disclose their data collecting activities. As noted previously, many online services are not currently disclosing their data collection activities.

B. Reasonable Data Security Practices

Proposal: Require entities to establish "reasonable" security measures to safeguard sensitive personal information.

Illinois law does not specifically require data collectors to secure the personal information they collect. When a data breach impacts Illinois residents, the office uses its authority under the Consumer Fraud and Deceptive Business Practices Act to examine the company's data security practices.[45] Although this authority is sufficient to find that an entity's

[45] 815 ILCS 505/1.

poor security practices constitute an "unfair or deceptive business practice," affirmative obligations on entities to protect personal information strengthen the office's authority and encourage companies to adopt stronger data security provisions. The provision would also send a clear message that any information covered under the definition of "personal information" must be protected.

This requirement should be achievable for entities collecting personal information because many are already complying with "reasonable" data security requirements at both the state level and federal level.

1. Examples at the State Level

Eight states have enacted a reasonable data security standard: Arkansas, California, Connecticut, Florida, Maryland, Nevada, Texas, and Utah.[46] These states require companies to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Below is a sample of these statutes.

- **California:** A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Cal. Civ. Code § 1798.81.5.

- **Florida:** Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information. Fla. Stat. § 501.171(2).

- **Maryland:** To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. Md. Comm. Law Code § 14-3503.

2. Examples at the Federal Level

The Federal Trade Commission has also repeatedly asserted in testimony before congressional committees that it supports a requirement for reasonable security measures. In 2014, before the Senate Commerce Committee, the FTC stated:

> The FTC supports federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate

[46] Ark. Code § 4-110-104(b); Cal. Civ. Code § 1798.81.5; Conn. Gen. Stat. § 42-471; Fla. Stat. § 501.171(2); Md. Comm. Law Code § 14-3503; Nev. Rev. Stat. § 603A.210; Tex. Bus. and Comm. Code. §521.052; Utah Code § 13-44-201.

circumstances, to provide notification to consumers when there is a security breach. **Reasonable and appropriate security practices** are critical to preventing data breaches and protecting consumers from identity theft and other harm.

Additionally, federal rules, in specific circumstances, already require "reasonable" data security measures. For example, the FTC's rule for the Children's Online Privacy Protection Act (COPPA) includes a requirement that operators of websites for children "**must establish and maintain reasonable procedures** to protect the confidentiality, security, and integrity of personal information collected from children."

3. U.S.-EU Safe Harbor Agreement

Because the European Union has much stronger privacy protections for its citizens than the United States does, the United States government had to agree to create a "Safe Harbor" Framework through the Department of Commerce before U.S. companies could transfer the data of European citizens. Companies participating in the U.S.-EU Safe Harbor Framework must publicly declare that they are in compliance with the Framework's requirements. Among the requirements is the obligation that "[o]rganizations must take **reasonable precautions** to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction."

This commitment to "reasonable precautions" is important because nearly 4,000 U.S. companies, including more than 200 headquartered in Illinois, have made the commitment in order to transfer the data of European citizens. As a result, companies in the United States are often already providing "reasonable" data security protections for citizens of foreign countries.

C. Notification

Proposal: Expand the definition of personal information.

Proposal: Require entities to notify the Illinois Attorney General's office when breaches occur.

Proposal: Enable small businesses to notify local media, rather than statewide media, when breaches occur.

PIPA has not been significantly amended since it was first passed in 2005. As a result, many other states now have data security laws and data breach laws that are more protective of consumers than Illinois law. Compared to many states, the law on data breach notification in Illinois is narrow in what it covers. Currently, an Illinois resident is only notified of a data breach if his or her name is breached along with his or her (1) driver's license number, (2) financial account number, or (3) Social Security number. Many states now have a much broader definition of breached "personal information" that triggers a notification requirement.

When Illinois passed its law in 2005, understandably, the harms to consumers that policymakers most feared were fraud and identity theft. PIPA's triggers for data breach notification reflect this focus. While these harms continue to be the most significant potential damage from a data breach, as consumers' use of the Internet has grown since 2005, the manner

in which they can be harmed has expanded. Increasingly, data breaches have the potential to cause reputational harm as well.

Some of the amendments that other states have made to their data security laws, as well as the changes that the office is proposing, reflect this shift. As discussed further below, it is the office's view that a data breach of sensitive, personal information should be treated as potentially harmful to consumers, whether or not that breach leads directly to financial harm via fraud or identity theft.

1. Expansion of the Definition of Personal Information

a. Encryption Key

PIPA currently requires notification of a breach of personal information when "either the name or the data elements are not encrypted or redacted."[47] This safe harbor for encrypted information has been successful, as it encourages companies to take the step to encrypt information that would otherwise trigger notification requirements. However, the provision, as it is currently drafted, does not cover very plausible situations involving breaches of encrypted information that have occurred. The law does not address breaches where the information was encrypted or redacted, but the key to unencrypt or unredact the data was also compromised. In such a circumstance, it does not matter that the data was encrypted or redacted because the consumer's information is readable.

The office proposes to revise the definition of personal information to include breaches where the keys to unencrypt or unredact the data are compromised along with encrypted or redacted data.

b. Username/Email and Password (Login Credentials)

Login credentials for accessing online accounts – user name or email address and password – are not covered under the Illinois breach statute. This limitation in Illinois law means that breaches of very sensitive online accounts may go unreported to Illinois consumers. Breaches of this kind can be very damaging to consumers because: (1) online accounts are often tied to financial accounts; (2) online accounts often hold very sensitive data about consumers; and (3) breached online accounts are used by hackers to perpetuate phishing and spam e-mail schemes.

i. Financial Information

Many online accounts that consumers use on a regular basis also hold their financial account information. While this practice is very beneficial to consumers because it enables them to make purchases without reentering their financial account information every time they make purchases via trusted websites, it also means that a hacker with access to a username and password can make fraudulent purchases with their accounts. This manner of fraud via online accounts is not a hypothetical fear—it is already occurring. In addition to the possibility of fraud through financial accounts, fraud through other online accounts can occur. For example, United

[47] 815 ILCS 530/5.

Airlines recently announced that hackers had stolen the login credentials for fliers with airline miles accounts. The hackers used the miles to make fraudulent purchases.

ii. Sensitive Information

Consumers store other types of sensitive information in their online accounts as well. This practice has expanded as cloud computing has grown more reliable and become cheaper to use. Rather than save files on hard drives, consumers can now store documents, email, photos, and videos via low-cost, online accounts. Yet, despite the sensitive nature of the information stored in these accounts, companies have no responsibility in Illinois to notify consumers if the login credentials are breached.

iii. Perpetuating Phishing and Spam

The combination of a user name or email and password can also cause harm because consumers frequently use the same access credentials for multiple sites. Access to one account can usually expose sensitive information about the consumer via additional accounts.

Krebs on Security, a well-respected website on data security created by a former *Washington Post* journalist, reported last year that hacked login credentials for popular sites like iTunes, FedEx.com and United.com were being sold for $6-8 per account on the black market.[48] As the post noted, "even if your email isn't tied to online merchants, it is probably connected to other accounts….They are harvested for the email addresses of your contacts, who can then be inundated with malware spam and phishing attacks."[49]

If companies notify consumers when their login credentials were breached, it will encourage consumers to change their passwords, which will reduce the harm from the breach. Additional transparency on such breaches would also encourage consumers to change their passwords regularly.

c. Biometric Data

The use of biometric data (e.g. fingerprints, retina images) as an access credential is becoming increasingly common. The most recent iPhone, for example, offers the use of a fingerprint for login authentication. Yet, if a fingerprint were to be stolen in a breach, that consumer would forever be at risk when they used their fingerprint in any other system. Additionally, they may be susceptible to future types of identity theft.

Unlike a password, a consumer cannot change their fingerprint after a breach. But they can alter their privacy settings to no longer allow access without some other identity verification (multifactor authentication) or prohibit access via fingerprint altogether. Notice of a breach of biometric data would prompt consumers to take such action. It would also incentivize companies to secure this data so that they can avoid the financial and reputational costs of losing such sensitive information.

---

[48] KrebsonSecurity.com, "The Value of a Hacked Email Account," June 10, 2013, available at: http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/.

[49] *Id.*

d. Medical History and Health Insurance Information

The office proposes expanding the definition of personal information to include medical information (information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional) and health insurance information (an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals record).

Medical history and health insurance information are currently covered under the federal breach notification rule of the Health Information Technology for Economic and Clinical Health (HITECH) Act[50] and the FTC's Health Breach Notification Rule. [51] However, they are not protected by state law. Additionally, consumers are now sharing many types of medical information outside the scope of HIPAA, most frequently via websites and apps. The proposed expansion would protect this information.

e. Geolocation Information

As discussed above, with the rise of geolocation capabilities on smartphones, entities now have access to very detailed data about consumers' movements. While breached geolocation data is less likely to lead to identity theft, it could very likely lead to reputational harm and cause other damage to affected individuals. Furthermore, location information from smartphones can be used to stalk, harass or inappropriately monitor individuals. Given how sensitive this information is, entities that collect it should take reasonable steps to protect the data, and if unauthorized access to this information occurs, consumers should be notified.

f. Consumer Marketing Information

When using the Internet or smart phones, consumers also generate other types of sensitive information, including information related to transactions, searches, and browsing habits. Marketers and data brokers use this information to build profiles on consumers. While this information may not lead to identity theft or fraud, a breach of such information could be incredibly damaging if it was connected to an individual's name. Consequently, entities with this information should take reasonable steps to protect it, and consumers should be notified when unauthorized access to the information occurs.

g. Contact Information Combined with Identifying Information

Consumers' contact information has repeatedly been part of data breaches that have occurred in recent years. However, there is no requirement to notify consumers when a breach of contact information occurs. Historically, the viewpoint has been that consumers should not be notified of such breaches because their contact information is already public, and consequently, that information cannot harm them. Yet, the rise of phishing attacks has shown that consumers can be targeted when hackers know specific pieces of information about them. Additionally,

[50] 42 U.S.C. § 17932.

[51] 16 CFR § 318.2 (referencing 42 U.S.C. § 1320d(6)).

contact information, combined with identifying information—like mother's maiden name and date of birth—can make it easier for hackers to access consumers' online accounts. For these reasons, the office believes consumers should be notified when their contact information is breached along with either their date of birth or their mother's maiden name. Consumers affected by such breaches are more susceptible to fraudulent activity and identity theft, and they should be given the opportunity to take steps to protect themselves.

2. Notification to the Illinois Attorney General's Office

Under PIPA, data collectors have no obligation to report a data breach to the Attorney General's office. As a result, the office usually learns about breaches from media reports or other states, which puts it at a disadvantage when responding to large data breaches. If a breach notice is sent to Illinois residents, but is not covered by the news, the office may never hear about it.

Requiring data collectors to send breach notices to the Attorney General's office would significantly improve its ability to quickly respond to breaches. The office could use these notifications to triage and more effectively focus our investigative efforts – and those of the multistate working group – on those breaches that are the most significant.

Additionally, a reporting requirement to the office would enable it to become a repository of data breaches for Illinois residents. If given this authority, the office intends to create a website that lists the data breaches that have affected Illinois residents. As mentioned above, at roundtables, the office frequently heard from consumers stating that they did not know where to find information about breaches that have occurred. The California Attorney General's office currently posts a list of the data breaches that it is notified about[52] and the Illinois Attorney General's office could easily do the same if given similar authority.

While large breaches generate significant media attention, smaller breaches do not. Consequently, with respect to small retailer breaches of payment card data, many Illinois residents are very likely unaware that their information was compromised. The proposed website could address this problem.

3. Small Business Notification Exception

Data breaches that have occurred this past year have shown that some small businesses suffering breaches are too small to provide effective notice of a breach to consumers pursuant to PIPA. For example, if a small business suffers a breach and does not have the affected customers' contact information, the small business can comply with the act by notifying "statewide media." However, the likelihood that "statewide media" will run a story based upon a breach at one location in one town is small. For that reason, the office suggests allowing entities, like small businesses with one location, to notify "prominent local media" in areas where affected individuals are likely to reside, if such notice is reasonably calculated to give notice to persons whom notice is required.

[52] State of California Department of Justice, Office of the Attorney General, "Search Data Security Breaches," available at: oag.ca.gov/ecrime/databreach/list.

VI. CONCLUSION

Data security is a significant challenge for consumers, government, and the private sector in the Digital Age. This challenge can only be overcome through a coordinated effort at all levels of government that acknowledges the roles of both consumers and data collectors. To do that, consumers and data collectors need more transparency over the vulnerabilities that are being exploited and the breaches that are occurring. The recommendations in this report will help us achieve these goals and, in so doing, will help ensure better security for consumers' sensitive, personal data.

Illinois Attorney General Consumer Fraud Hotlines

Chicago	**Springfield**	**Carbondale**
1-800-386-5438	1-800-243-0618	1-800-243-0607
TTY: 1-800-964-3013	TTY: 1-877-844-5461	TTY: 1-877-675-9339

Identity Theft Hotline

1-866-999-5630
1-877-844-5461 (TTY)

Línea Gratuita en Español

1-866-310-8398

www.illinoisattorneygeneral.gov

Printed by the authority of the State of Illinois.
This material is available in alternate format upon request.