Personally Identifiable Information and New Privacy Laws

A White Paper by
James Harrison, RCE, CAE
President and CEO of MLSListings Inc.

September 2018

INTRODUCTION

Imagine a vendor saying that "we pay to get the data from the MLS; therefore, the data is ours and no privacy or security issues are at play because the data is not private identifiable information if we bought it." Some may think this scenario is too far-fetched, but it is not. It actually happened, and it illustrates how much confusion exists over personally identifiable information (PII) and privacy and security concerns.

This white paper is an attempt to explain pertinent issues and offer proactive steps that MLS companies and real estate brokers can take to minimize the potential harm resulting from the mishandling of PII.

WHAT IS PII?

PII is any data that could potentially identify a specific individual. Some examples are name, social security number, date and place of birth, mother's maiden name, photo, fingerprint, bank account, postal address, email address, phone number, and employment information. One type of PII especially relevant in the real estate industry is a paragraph that gives a personal description of the agent, including spouse, children, pets, areas of specialty, etc.

MLS LISTINGS

ISSUES

The consequences of mishandling PII can be severe. In the case of Facebook, concerns over how the company handles users' private data led to a 20 percent drop in value of that publicly-traded company during February and March of 2018.

Data breaches, the intentional or unintentional release of PII to an untrusted environment, are becoming increasingly common. A data breach from an MLS or a brokerage could result in substantial fines and restitution, but beyond the immediate financial impact, it could hurt the company even more drastically in terms of cost to the company's "image" and "future revenue lost." Beyond fines and other payments, MLS of choice would likely lead many customers to move to a neighboring MLS. The MLS dealing with the breach would thus lose a substantial amount of subscription fees revenue.

Consider an agent whose email was secured with a nearly impenetrable password only to have a hacker use "social engineering" to crack the agent's password. If that PII could be social engineered to help crack a password, then it could cause customers to second guess what data they should be putting on the MLS. With less data on the MLS, the MLS becomes less valuable, making customers use it less.

In addition, increasing publicity over data breaches is causing a growing number of subscribers and consumers to demand that MLS companies and brokers redact their information from their systems. As a result, many companies are developing new terms of service that define how they use subscribers' data.

Furthermore, there was a great deal of attention in early 2018 when the European Union's General Data Protection Regulation (GDPR) took effect. While the rules and laws around privacy differ from state to state and country to country, it is advisable for MLS companies and brokerages to act not because of what local, regional, or national laws require, but to act instead because of what it would mean to the business if there were a breach of security and PII was released into the wrong hands.

NALLY
IFIABLE
MATION

BEST PRACTICES TO SECURE PRIVATE INFORMATION

MLS companies and brokerages need to take several actions in this regard, including:

1. **Having a crisis plan.**

Even in the best conditions, breaches happen. To prepare for such an incident, MLS companies and brokerages should know in advance what they are going to do: Will they notify people? Who will they notify? How will they notify them? Who in their organization will be in charge in such a crisis? Having a crisis plan specific to a data breach is key to being able to execute on that smoothly if it were to happen at some point.

2. **Employing data mapping.**

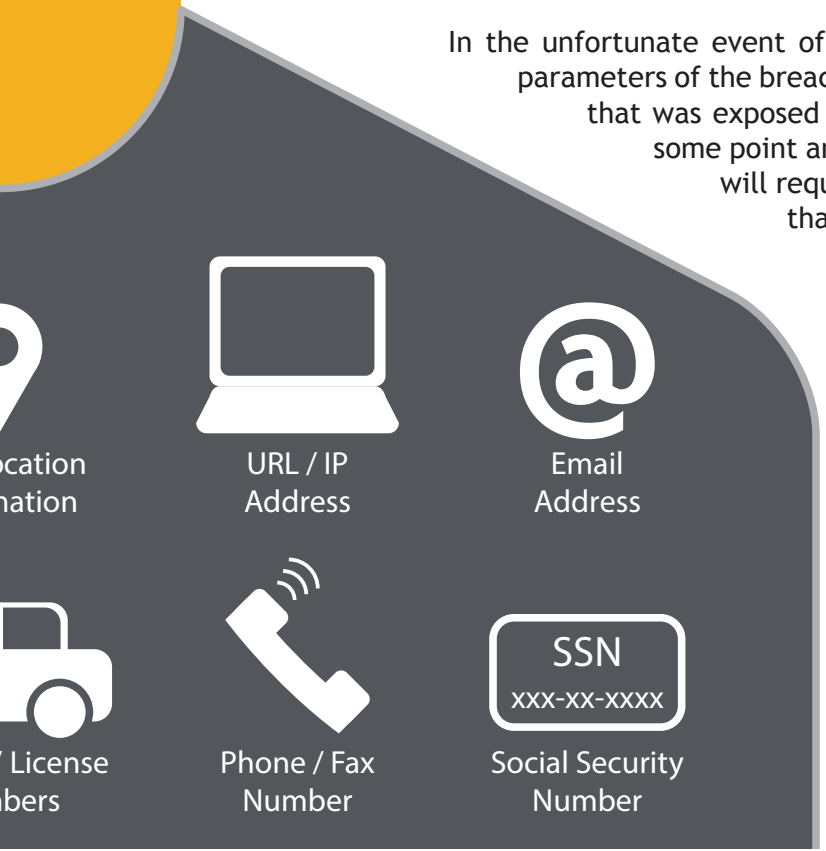
As part of the MLS company's or brokerage's preparation, a crucial step is to understand what PII exists in that company's system, and the best way to do that is by creating a "data map." The company will want to know what PII that is and then learn how it was obtained. It requires knowing the types of people for whom the company has PII: current employees, former employees, customers, and consumers, for example. The company will also want to know for each of those types of people where the data comes in, where it flows, and how it is stored. Was it obtained through a tool that somebody entered information into? If so, who entered that information, where did that information get stored, and where does that information go after it is entered into the tool?

Data mapping requires putting a process in place so that as new data is added into the company's system or the data in the system changes, there is a method for updating those maps so they are always current. The process will involve meeting with IT staff to understand where all that data resides and how it is being protected. It bears noting that the data must be protected by traditional firewalls and encryption in a database.

In the unfortunate event of a breach, after company executives determine the parameters of the breach, the data map readily shows the type of information that was exposed and the people who had that data exposed. Also, at some point an employee, former employee, customer, or consumer will request a change in how a company maintains their PII. In that case the data map will allow the company to easily respond because it tracks all PII the company holds, where it is stored, and how it is secured.

3. **Monitoring those accessing the company's listings.**

It is important to know who is monitoring this data and how it is being monitored to be aware if a breach occurs. The industry standard is to employ state of the art real-time monitoring and remediation in case of a breach. A third-party vendor may be used if a company lacks the internal means to manage this.



4. Transmitting listings only to approved third parties.

As a routine part of doing business, MLS companies transmit to approved brokers and technology companies that publish their listings. It is a good practice for MLS companies to only send to approved vendors, and on a regular basis to have a compliance team confirm that the data is only going to those approved locations. In the event that data is going to a vendor that was not approved, the company must investigate how the data was "leaked."

5. Requiring rigid authentication to access the company's system.

To ensure that the MLS company's listings are accessed only by those whom the company chooses, it is important to install a number of controls to ensure that only the correct people have access. The process must be controlled tightly enough so that agents complain on occasion about how difficult it is to access the company's system.

6. Demanding vendor compliance.

MLS companies and brokerages must educate vendors to make sure all vendors understand privacy and data security, and the companies and brokerages must demand that the vendors show proof of compliance with all laws. The company must update contracts with all vendors to reflect that demand and ensure requirements are met. This will safeguard against the scenario described at the beginning of this white paper. If a customer's data is hacked because of the poor actions of one of the company's vendors, it will be the company's business reputation on the line even though it was a vendor that compromised the customer's data.

7. Having good data retention policies.

Another action to reduce a company's risk of exposure around PII is to have a clear plan regarding when to purge data. It will reduce the amount of PII in the company's system and help minimize the company's risk. Time frames for how long a company should retain PII data for ex-employees, customers or subscribers, and consumers are best determined by each company's needs.

CONCLUSION

Managing PII is not easy, but it is a critical responsibility and a smart business activity. In this new landscape, with the challenges currently facing our industry, it is certainly worth the effort. Those who do not look at the PII issue now are almost certain to have to look at it in the future.

MLSListings Inc. is recognized as a premier multiple listing service in the nation. Based in the heart of Silicon Valley and specializing in Monterey, San Benito, Santa Clara, Santa Cruz, and San Mateo Counties, MLSListings provides real estate professionals and consumers with accurate data that is updated every five minutes. Facilitating more than $70 billion in annual real estate activity, the MLSListings platform is the intersection of comprehensive real estate data and the transaction for the Northern California marketplace.

MLSListings Inc.
740 Kifer Road, Sunnyvale, CA 94086
(866) 734-5787 | support@mlslistings.com
www.mlslistings.com