NATIONAL ASSOCIATION of REALTORS®

500 New Jersey Avenue, N.W.
Washington, DC 20001-2020
202.383.1194 Fax 202.383.7580
https://www.NARrealtor/political-advocacy/federal-advocacy

John Smaby
2019 President
Bob Goldberg
Chief Executive Officer

ADVOCACY GROUP
William E. Malkasian
Chief Advocacy Officer/Senior Vice President

Shannon McGahn
Senior Vice President Government Affairs

HEARING BEFORE THE SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION SUBCOMMITTEE ON MANUFACTURING, TRADE AND CONSUMER PROTECTION

ENTITLED "SMALL BUSINESS PERSPECTIVES ON A FEDERAL DATA PRIVACY FRAMEWORK"

STATEMENT FOR THE RECORD OF

THE NATIONAL ASSOCIATION OF REALTORS®

MARCH 26, 2019

INTRODUCTION

Chairman Moran, Ranking Member Blumenthal, and members of the subcommittee; my name is Nina Dosanjh. I am a REALTOR® and the Director of Strategic Alliances and Technology with Vanguard Properties in San Francisco, California. I serve as the 2019 Vice Chair of the National Association of REALTORS® (NAR) Federal Technology Policy Committee. I am here today to testify on behalf of the 1.3 million members of the National Association of REALTORS®

In my role at Vanguard, in addition to being an active real estate agent, I am responsible for analyzing existing partnerships and identifying new alliances to benefit the brokerage, its agents, and the consumer. I am responsible for researching and suggesting improvements to operational systems and technology products for the firm's agents. Vanguard Properties operates twelve offices in the San Francisco bay area with nearly 400 agents. While my brokerage is larger than the average REALTOR® business, my leadership role at NAR and engagement with fellow real estate professionals enables me to be very familiar with the impact of potential privacy legislation on small REALTOR® businesses.

REALTORS® SUPPORT CONSUMER PRIVACY

REALTORS® have no higher priority than their relationships with their clients and the protection of their clients' best interests. As a result, REALTORS® have a long history of supporting efforts to protect consumers' sensitive personal information. The REALTOR® Code of Ethics and Standards of Practice explicitly acknowledge a REALTOR's® obligation to preserve the confidentiality of personal information provided by clients in the course of any agency or non-agency relationship – both during and after the termination of these business relationships. Protection of client personal information is an important part of the trusted relationship our members enjoy with their clients and that clients expect throughout their real estate sales transaction.

NAR provides extensive resources and training opportunities to members on data privacy and security, stressing the importance of safely collecting and retaining information from clients and safeguarding their own businesses' sensitive information. NAR provides our members with online training, videos and toolkits all in an effort to help our members make privacy and data security a fundamental part of their business.

REALTORS®, like many main street businesses, rely on data to enhance revenue and drive efficiency, whether by better understanding the needs of existing customers, reaching new ones, or obtaining valuable insights to guide a wide array of business decisions. For example, REALTORS® may use consumer data to allow them to advise their selling clients on how to price their home and how many potential buyers will be interested at different price points. It can also be used to give buyers a better sense of what types of properties competing home buyers are looking at, as well as their buying ability. In sum, REALTORS® use the consumer data they collect to improve their clients experience in a way that consumers can understand and expect. Our members are not in the business of selling consumer data to third parties.

THE MAJORITY OF REALTORS® OPERATE SMALL BUSINESSES

Real estate firms vary widely in size, but the overwhelming majority is composed of very small entities. NAR's most recent surveys indicate that more than half of all residential real estate firms have less than twenty-five agents, and the typical sales agent is affiliated with an independent firm with only one office. As a result, these businesses lack the staff that a larger corporation has to dedicate to regulatory compliance.

Most real agents affiliated with residential real estate firms in the US are independent contractors. In fact, 9 out of 10 NAR members are independent contractors. Any new data privacy requirements will impact the individual real estate agent who is a legal business entity separate from the real estate company with which they are affiliated. As independent contractors and small businesses, real estate professionals and firms lack teams of compliance personnel necessary to keep pace with complicated and potentially burdensome regulations. Given these characteristics of the real estate industry, NAR's top priority for any new federal privacy law is ensuring that Congress craft realistic compliance requirements for small businesses and independent contractors.

KEY PRINCIPLES FOR FEDERAL PRIVACY LEGISLATION

Considering that the protection of consumer data privacy is a priority issue for Congress, and should be for all businesses and consumers across the nation, NAR supports six key principles in federal privacy legislation with the aim to establish a uniform, nationwide and consumer-centric data privacy law:

Establish Uniform Standards for Businesses and Equal Protection for Consumers
Federal law should provide consumer data with uniform legal protections across all industries. Any federal data privacy legislation should apply requirements to all industries that handle personal data and not exempt certain sectors of the economy from providing consumer data protection. The level of protection for data should not depend on arbitrary distinctions between industries, such as whether a business directly collected data from a consumer or obtained it in a business-to-business transaction. Businesses that obtain consumer information indirectly should have the same obligations and responsibilities to protect that information as the businesses that obtain consumer information directly.

Direct Statutory Obligations for All Service Providers Handling Consumer Data
Effective consumer protection regulations cannot be achieved by relying on some businesses to regulate the conduct of other businesses through contracts alone. For example, small businesses and independent contractors may lack experienced personnel, legal expertise, bargaining power or business contract sophistication to negotiate terms to require larger businesses to adequately protect the smaller business's customer data when it is in the larger business's possession. Such data service providers, particularly those offering transmission, storage, analytical processing or other consumer data services for thousands of small businesses, need direct statutory obligations to ensure they comply with relevant laws to govern customer information.

Small businesses and independent contractors, such as those operating in the real estate industry are often in substantially the same position as an individual consumer when negotiating a contract with a large service provider. Ultimately, we are left with only two choices use the service under their standard terms or go without such services, directly harming the business and its clients. Expecting

small businesses to effectively negotiate contract terms surrounding privacy and data security on their own against large corporations with extensive legal departments is simply not a viable option.

Transparency and Customer Choice
Consumers deserve to know what categories of personal data that businesses collect and how that data is generally used by them. These policies should be clearly disclosed in company privacy policies and readily accessible to consumers looking to learn how their data is collected and used by the business providing the goods or services. Federal data privacy law should provide the regulatory flexibility necessary to ensure that transparency in privacy policies is provided to consumers without unnecessarily burdening businesses with requirements to seek consumer consent when they are continuing to use data based on reasonable consumer expectations.

Accountability for Business's Own Actions
Privacy legislation should not include terms that could potentially expose businesses to liability for the actions or non-compliance of a business partner. Those business partners should be responsible for their own compliance and any resulting liability. In particular, consumer-facing businesses should not be unfairly saddled with liability if partner businesses do not fulfill their own obligations under the law.

Uniform Nationwide Standard and Enforcement for Data Privacy
Congress should create a sensible, uniform federal framework for data privacy regulation that benefits consumers and businesses alike by ensuring that sensitive consumer information is protected in a consistent manner regardless of the state in which a consumer resides. Preempting state laws effectively setting an alternative set of nationwide rules is necessary to achieve the important, national public policy goal of uniformity while at the same time providing businesses operating in multiple states the confidence of consistency for their consumer transactions. Consumers will likewise be confident that their data is protected regardless of where they live or travel.

Reasonable FTC Enforcement Authority
The Federal Trade Commission (FTC) should have the appropriate authority to enforce comprehensive privacy regulations. NAR appreciates that the FTC employs a scalable reasonableness approach that determines the appropriateness of business practices in light of the size of the business and the sensitive nature of the data they process under Section 5 of the FTC Act. Any future privacy legislation should ensure that the FTC continues to employ flexibility in their implementation of reasonable privacy standards that will permit the Commission to enforce such regulations fairly and equitably to ensure businesses' compliance with them and to promote robust consumer protection.

Concerns with the California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA) is a sweeping privacy law that will provide consumers with a number of new rights regarding their personal information but hamstring businesses seeking to ensure compliance. It is important to note that the impetus behind CCPA was the concern over the use of consumer data by internet, technology and media companies, but the breadth of the law as currently written is likely to sweep in many small businesses that were never considered to pose a threat to consumer privacy. As a result, the CCPA raises significant questions and concerns for

REALTOR® businesses that we believe merit the Committee's attention so that any new federal legislation does not duplicate the unintended consequences brought about under CCPA.

Small Business Exemption
The CCPA attempts to exempt small businesses from its application. It limits application to those businesses that meet one of three criteria 1) has gross annual revenues of more than $25 million, or 2) derives half of its revenue from the sale of consumer data, or 3) buys, sells, shares or receives for its commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices. The third criteria could sweep in small REALTOR® businesses and require them to comply with all of the provisions of the CCPA.

For example, if a consumer visits a REALTOR® website using a cellphone, a home PC and a work PC while searching for a home, which is a very common scenario during the homebuying process, then that business would have collected the personal information of one consumer from three devices. Under criteria three above, it has been calculated that the collection threshold of 50,000 consumers/households/devices equates to only to 137 visits to a website on a daily basis. This can cumulatively be met by a small number of individuals. Thus, any business operating on the internet today can easily meet this 50,000 threshold regardless of the size or sophistication of that business.

This points out that Congress must carefully consider small business thresholds and narrowly tailor covered entity definitions in any new privacy legislation to both the size and scope of the businesses as well as the sensitive nature of data collected. Mere records thresholds are inadequate.

Impact of Right of Deletion on Multiple Listing Services (MLSs)
The Multiple Listing Service (MLS) serves as the real estate industry's internal highway, transporting data between brokers and agents. MLSs organize property listing information in a common database resulting in lower search costs, greater exposure of inventory to potential buyers, and easy market entry for new brokers large or small to compete. As a result, the MLS is critical to the home buying and selling process. Questions raised by how the CCPA will be enforced have important implications for MLS businesses. The CCPA grants consumers a right to request deletion of their personal information from businesses covered by the Act. Given the very broad definition of personal information and questions surrounding the "publicly available information" exemption, there is a possibility the CCPA, would provide a consumer the right to request the deletion of the sale price of their home from the MLS. This would result in a dramatic threat to the ongoing operation of the MLS as the comprehensive source for real estate listing data in a market area. The fallout from this loss of data would have far reaching implications beyond just REALTORS® and the MLS, as its role in determining valuation is relied upon by lenders and others in the greater real estate market and housing sphere.

Broad Definitions
The Definition of "Personal Information" is extremely broad. It covers information that "relates to, describes, [or] is capable of being associated with, or could reasonably be linked… with a particular household." This could be the case where the same IP address or delivery address is linked to multiple online accounts, creating difficulty responding to individual rights requests from one member of a household but not others. Thus, clarity and precision in the definition of personal information in any federal privacy legislation is critical for REALTORS® and other businesses to build effective privacy compliance programs.

The CCPA defines a "sale" of personal information" in a manner that captures any arrangement in which a business not only sells but "rent[s]" or "mak[es] available" personal information "for monetary or other valuable consideration." The breadth of this definition captures many types of data-sharing arrangements that are necessary in today's business environment and are not viewed by consumers as a "sale" of data. For example, REALTOR's® may share data with vendors to help market a client's home or to determine a competitive sales price. Congress should therefore be mindful of the importance of seamless data flows among business partners in order to deliver the efficient experiences our consumers demand from u

Conclusion

On behalf of NAR, I thank you for the opportunity to testify today. We urge you to consider these key principles and considerations as you develop federal privacy legislation. We especially thank you for considering the impact of such legislation on small businesses. NAR wants to ensure that any federal legislation on data privacy protects consumers in a nationwide, uniform and consistent way and in a manner that will not impose undue burdens on our small business members. We look forward to working with you in a constructive way during the 116th Congress.