US Data Privacy Laws:
Legal and Marketing Professionals' Views

Research Paper

May 2013

IDG Connect has produced new research based on marketing and legal professionals' views of data privacy laws in the US. This sets out to address how the two groups feel about the current state of data privacy legislation and whether there is a disconnect between the two departments.

Contents

US Data Privacy Laws 3

A Mess of Legislation 4

Legal Professionals vs. Marketers 5

US vs. EU 7

Conclusion 8

US Data Privacy Laws: Legal and Marketing Professionals' Views

The last few years have seen a surge in the volume of data that organizations hold on individuals, and now, the way marketers communicate with their lists is often subject to legislation. This means marketing and legal departments have to work closer than ever before. However, beyond this, privacy is an issue that impacts everyone. And most people have a personal opinion on the kind of information that many companies own about them.

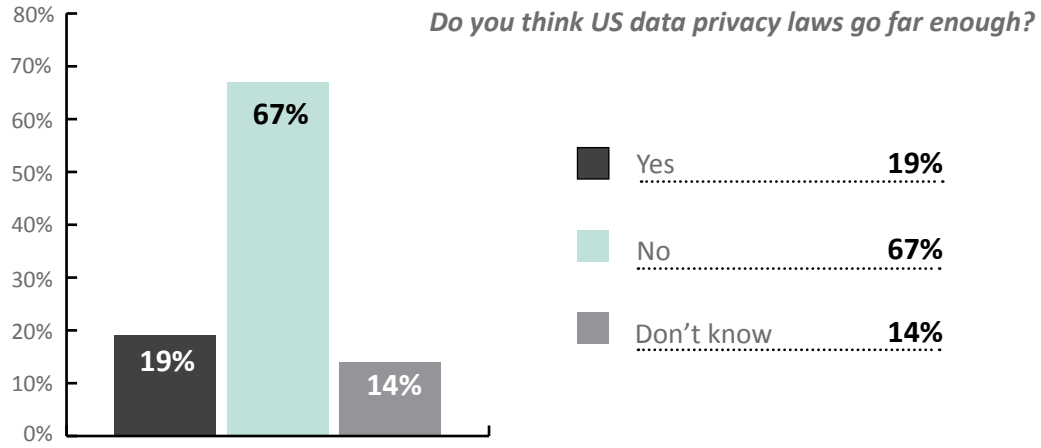
In a bid to explore this further, IDG Connect has produced new research on marketers' and legal professionals' views of data privacy. This sets out to address how these groups feel about the current state of data privacy and whether there is a disconnect between the two departments.

"Now that modern devices afford abundant opportunities for the perpetration of such [privacy] wrongs without any participation by the injured party, the protection granted by the law must be placed upon a broader foundation." (Warren & Brandeis, 1890)

These words may be over a hundred years old, but they are as true today as when first written, and with the orientation vote imminent in the LIBE on Europe's General Data Protection Regulation, the United States' patchwork of data privacy laws has come under renewed scrutiny.

Warren and Brandeis' hallmark article in the Harvard Law Review in 1890 is generally considered to be the basis for establishing the right to privacy as a tradition of common law. Thanks to technological advances, the "right to be let alone" has had to expand considerably and countries all over the world now specific legislation addressing the privacy of data. But do data privacy laws in the United States go far enough?

Our survey of 40 legal professionals and marketers across the US showed that an overwhelming majority (81%) of those we asked either didn't think US privacy laws were sufficient, or didn't know for sure. One respondent went so far as to claim, "I don't believe there is any privacy… Companies and individuals are being hacked at an alarming rate even with all the protection they think they have so there is little to no privacy or safety there." Only 19% of legal professionals and marketers that we surveyed felt that US privacy laws go far enough, and those that did tended to be much more succinct with their comments: "I feel the laws are sufficient."



Interestingly, the two industries shared remarkably similar views, with only 18% of marketers and 20% of legal professionals agreeing that current US data privacy laws are adequate. This seems to be supported by our findings that a significant proportion (17%) of marketers do not consider themselves "extremely impacted" by data privacy issues – perhaps if they were, data privacy laws would be considered more effective? As one marketer put it: "If the consumer only knew the practices of some business – from marketers to businesses in the information collection business – there would be outrage."

In the course of this report we will outline current US data privacy laws and present our research into the opinions of legal and marketing professionals in an effort to discover whether US data privacy laws really are sufficient.

A Mess of Legislation

Unlike almost every country in Europe and most of Latin America, Asia and Africa, the United States doesn't have a single, comprehensive law on data protection and privacy. Instead, the country relies on a combination of federal and state laws and regulations, and self-regulation. But while companies can be penalized by the FTC for violating their privacy notices, violation is unlikely since the privacy notices are written by the companies themselves.

Privacy legislation in the US has often been adopted on an ad hoc basis: new legislation arises as its required (the Video Privacy Protection Act of 1988, the Cable Television Protection and Competition Act of 1992); different legislation exists for different industries (the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA)); and there's separate legislation covering data held by the government (the Privacy Act of 1974, the Computer Security Act of 1987). Many of the federal laws are specifically designed to protect personal data held by the federal authorities and, as such, don't have any authority over data collected, held, or used by non-government bodies.

This system appears to be geared towards a different world, because today, the big worry for individuals is the information that search engines and online companies like Google, Amazon and Facebook hold. Indeed, one respondent in the legal industry commented that, "personal data is a valuable commodity… the only way many companies (e.g. Facebook) will 'do the right thing' with regard to personal data is if the government puts laws in place requiring them to do so".

The key piece of data legislation in the US is the Privacy Act of 1974, which specifically governs the collection, maintenance and use of personal data held by federal agencies. The regulations cover disclosure, access, and amendment of data by an individual, as well as establishing a code of 'fair information practices'. Disclosure of information is prohibited without the written consent of the individual, except in the case of twelve statutory exceptions; individuals must be granted access to their records; and given the opportunity to amend those records if they can prove them inaccurate or irrelevant.

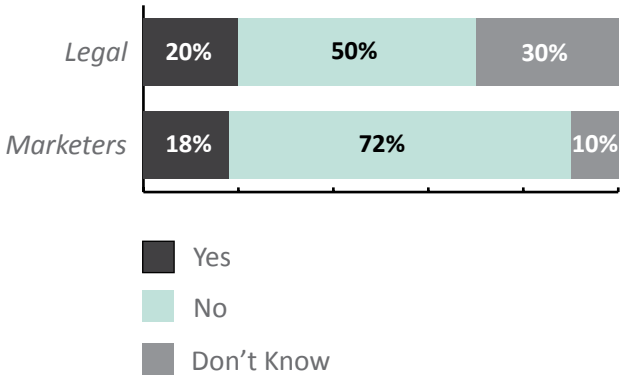
In 1988, the Privacy Act was amended to include The Computer Matching and Privacy Protection Act, with further amendments in 1990. The amendment improved protections for individuals whose records are used in automated matching programs by requiring a standardized procedure in carrying out matching programs; due process in order to protect subjects' rights; and the establishment of Data Integrity Boards at each matching agency to supervise matching programs.

As with many of the federal privacy laws in the United States, the Privacy Act only applies to records held by an "agency", meaning that any records held by non-agency entities are not covered. While there's a plethora of laws in the US that cover data privacy, the lack of a cohesive privacy law is seen by some as inadequate, as one legal professional put it, "US law is very limited and narrow in scope. There are many gaps where there is not law and many others where the law is uncertain."

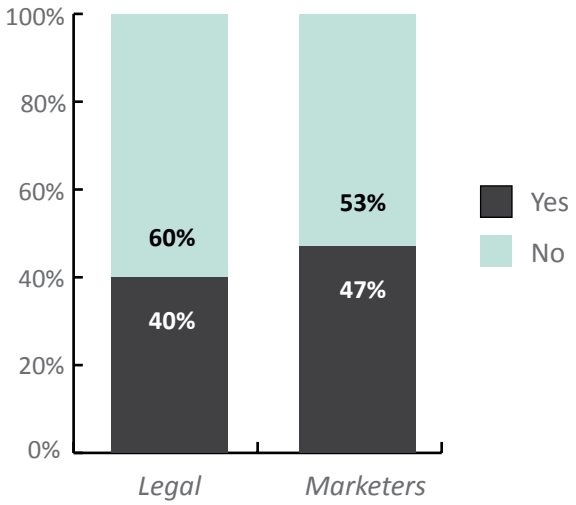
Legal Professionals vs. Marketers: Professional and Personal Opinions

We surveyed 40 legal and marketing professionals in the United States to find out whether they think current US data privacy laws are sufficient. The results were similar across the two professions, with just 18% of marketers and 20% of legal professionals of the opinion that privacy laws as they stand are adequate. The overwhelming majority of marketers (72%) thought that data privacy laws in the US do not go far enough; 50% of legal professionals agreed with this response, while 30% weren't sure. Some of those we surveyed openly admitted to not being sufficiently versed in US Privacy laws – "Not educated on the topic".

Do you think US data privacy laws go far enough?



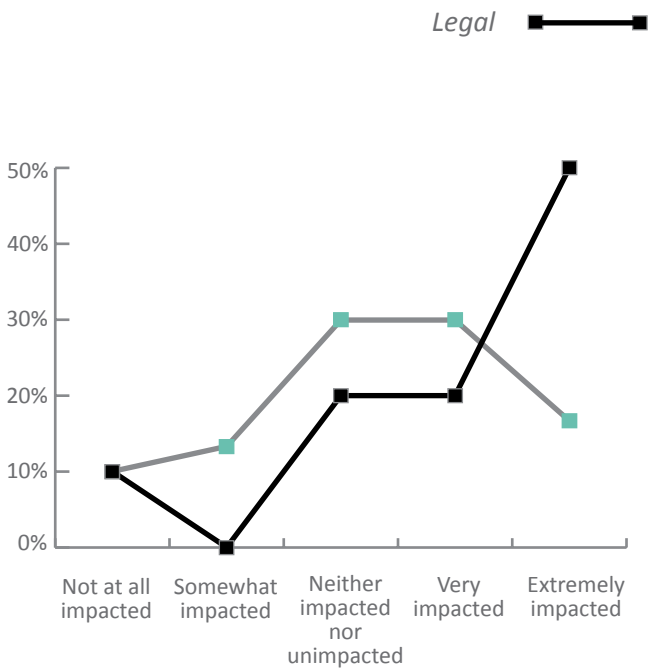
Is there ever a conflict between your personal views and professional experiences when it comes to data privacy?



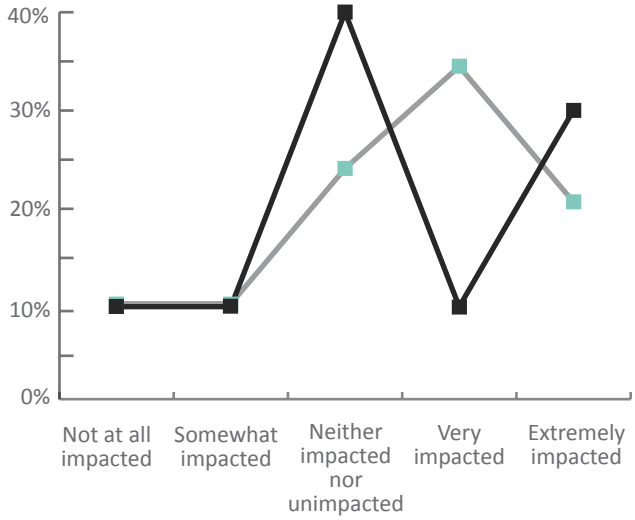
Marketers are well-known for using personal data in their professional lives, but do their personal and professional views on data privacy laws differ? Would you expect more conflict from a marketing professional than a legal professional? We found that the response from legal professionals was quite close, with 60% of respondents saying they didn't feel there was a conflict between their personal views and professional experiences when it comes to data privacy. We were surprised that the majority of marketers also responded in the negative (53% felt no conflict). However, one marketer was particularly strident in her view of their fellow marketers: "When it comes to business many, such as myself, will go above and beyond what is necessary to stay in compliance, but at the same time I find competitors take advantage of the weak, crossing the line in the sand which should be well established."

The responses of both legal professionals and marketers were varied when asked how they were impacted professionally and personally by data privacy issues. Our legal professionals were those most strongly impacted professionally by data privacy issues, with half of respondents saying they were "extremely impacted". The majority of marketers (60%) however, took a middle-of-the-road view of any professional impact. Neither industry seemed significantly impacted personally by data privacy issues, with just 33% of legal professionals and 20% of marketers claiming to be "extremely impacted". However, this may be a simple case of being unaware of any issues – as one legal professional commented, "I don't know if my data privacy has ever been compromised."

How impacted are you professionally by data privacy issues?



How impacted are you personally by data privacy issues?



The sufficiency of US data privacy laws for some respondents however, is not the main issue – the government that makes the laws is. One marketer explained, "Ironically, I find the US government is one of the worst violators when it comes to privacy and collection of information", while another held both the government and businesses to account, saying, "Too much snooping by the government, not enough honesty and transparency by businesses". Others believe that the government should stay out of data privacy all together, since it is down to the individual to protect their own data. Law enforcement was also accused of sidestepping privacy laws: "There are still too many people than can just say, 'I want this data, turn it over.' Even if they are law enforcement, they still need a warrant and a good reason, not just 'I think this person did something and I want to see what'."

US vs. EU: What Do the Differences Mean for Privacy?

Unlike the US, every country in the European Union adheres to the Data Protection Directive, a set of laws that protect an individual's privacy, and give them the means to take action if that privacy is violated. Furthermore, EU citizens' data is protected regardless of the industry, unlike in the US where a patient could sue their doctor for revealing personal information, but couldn't sue a website for revealing the same information. Despite this however, some of our respondents are happy with the US' current laws, with one saying, "I think US laws protect individuals sufficiently. I don't think the extra protection provided by the EU translate into *better* protection".

Debate has been raging on both sides of the Atlantic over the sufficiency of privacy laws in light of proposals currently before the European Parliament for the General Data Protection Regulation (GDPR). The GDPR will replace the current EU Data Protection Directive that doesn't take into account the effects of globalization and technological developments like social networks and cloud computing. The new legislation will not be limited to countries within the EU, but will also apply to all US companies processing the data of European residents.

If accepted, the law will prevent web businesses from performing basic collecting and profiling unless an individual gives their explicit consent. This will be a serious change because additionally, businesses will have to permanently delete personal information upon request, with the potential of a fine of up to 2% of their annual sales for not complying. The proposals are currently under consideration by the European Parliament, with adoption expected in 2014 provided that the provisions are agreed upon. The outcome of the parliamentary debate will be critical to technology companies in the US, since a third or more of their sales can be generated in the European Union.

The debate over the GDPR is not the first US-EU conflict over privacy and protection laws. When the EU Data Protection Directive was passed, it in theory prohibited the transfer of personal information from the EU to the US because the US does not have equivalent privacy protection in place. This is where the Safe Harbour framework came in. Described by Google as "a robust and highly successful privacy framework that has benefited consumers and our economies over many years", the US-EU Safe Harbor Agreement is designed to prevent the accidental loss or disclosure of information by enforcing adherence by US companies to seven principles. However, with Europe considering its new privacy policy, the US has raised concerns over what will happen to the Safe Harbour Framework and what effect it will have on businesses.

The Department of Commerce has announced clarifications regarding the US-EU Safe Harbor Framework and Cloud Computing that state as an officially recognised mechanism, approved by the European Commission, the Framework cannot be dismissed by the EU regulators. This may bring relief to those US companies that will be affected in a change in EU data privacy law, but is it the end of the matter? The Framework may be safe from complete elimination, but the European Commission is likely to reopen discussions about its content so they will more closely match the new legislation.

Conclusion

So what does the future hold for US privacy law? With the GDPR due for adoption next year, many companies in the United States are worried about the impact the stricter data privacy legislation will have on their business. But is stricter legislation necessarily better? While 81% of our respondents don't think so, some do, with one respondent going so far as to say that the laws themselves aren't the problem – "it's that the average consumer isn't aware of concerned as they should be. We need to raise consciousness to the problems and issues". So is that the simple solution – better privacy education? Given the speed of technological innovation this seems reasonable, after all, how can the law ever keep up with the speed of tech?

About IDG Connect

IDG Connect, a division of International Data Group (IDG), the world's largest technology media company, produces, publishes and distributes local IT and business information on behalf of a truly global client base. Established in 2005, we have a fully nurtured audience of 2.6 million professional decision-makers from 130 countries, and an extended reach of 38 million names. This lets us conduct research, create independent analysis and opinion articles, and drive long-term engagement between professionals and B2B marketers worldwide. For more information visit www.idgconnectmarketers.com