International Trademark Association

655 Third Avenue, 10th Floor
New York, NY 10017-5646, USA
t: +1-212-642-1700 | f: +1-212-768-7796
inta.org

Recommendations to Enhance Brand Value Through Data Protection

Prepared by the

Data Protection Committee – Best Practices Subcommittee

August 2018

TABLE OF CONTENTS

RECOMMENDATIONS TO ENHANCE BRAND VALUE THROUGH DATA PROTECTION

EXECUTIVE SUMMARY

The following report, prepared by the Best Practices Subcommittee of the Data Protection Committee, summarizes best practices for enhancing brand value in an era where data collection is temptingly common and commercially useful while carefully protecting brand equity and consumer trust. It points specifically to corporate policies and methods of security, data management and communications that must be implemented comprehensively in all corporate activities to safeguard brands and their relationships with consumers.

INTRODUCTION

A brand in many ways represents a relationship between customers and the brand owner. That relationship needs to be carefully managed. In the world of big data it is tempting to gather all available data and mine it in any commercially useful way. Fundamental aspects of the relationships with customers are at issue here and making mistakes that erode trust will inevitably erode brand value. A good example is a data breach which exposes customer data and is not handled correctly from a technical, legal or communication perspective. Another example is use of data in a way that is unauthorized or unexpected by the customer or even unethical, but nevertheless legal. This should not be solely a compliance driven issue but a central aspect of business strategy for brand owners to manage, so as to get the most from data assets without risking brand equity.

Through examination of major instances of data breach it can be concluded that many organisations suffer serious harm as a result of data breach incidents. For some corporations the breaches are on such a scale, or are handled in such a manner, that there is direct damage to relationships with customers and direct damage to the brand, share price and other measures of value. Case studies routinely show that a failure to follow best practices in security, data management and communication with affected parties and regulators causes and exacerbates the damage which can flow from data breach. Beyond instances of data breach, the otherwise lawful but unethical or unexpected collection and use of personal data can damage an organisations' relationship with its customers. In

order to best protect brand value, best practices need to be adopted as a matter of corporate culture, observed at all levels of corporate activity.

CORPORATE CULTURE

1. It is important that the corporate culture lives up to the company privacy and data protection policies.

2. Youth culture in many regions often has a more permissive attitude toward personal privacy and disclosing and sharing personal information. Education regarding privacy rights is a necessity.

3. Businesses should be mindful of data minimization principles since over-reaching requests for irrelevant or overly-broad information from consumers may damage goodwill and brand value.

SECURITY AND PREVENTION

4. Convey to internal teams any risks applicable in view of the nature and extent of any data collected or shared. Train employees on best practices for system and data security.

5. Preventing a data breach before it happens serves to protect the value of a company's trademark.

6. The timely deletion of data once it is not needed anymore helps to prevent a data breach or to limit its scope and builds trust with your customers.

7. Applying appropriate administrative, technical and physical measures to secure data is a key to building trust and confidence in your brand.

8. Track breaches, documenting causes of the breach, in order to improve security. Track contractual requirements to notify breaches.

9. Build an internal crisis management team to deal with a breach, whether it occurs directly without your business or at a third party with effects for your business. It is suggested to include representatives with decision-making authority from at least the following business areas: IT, Communications, Legal/Compliance and Controlling, in addition to the head of the affected department.

ADVERTISING AND PUBLIC STATEMENTS

10. Take a transparent, lawful and ethical approach to your use of personal information.

11. The circumstances, severity and likelihood of material harm in any data breach scenario will affect public messaging regarding the breach and the level of candor in that messaging. However, a commitment to improvement and learn lessons with regard to data security is vital in all data breach scenarios, even if customer data is not breached.

12. See data protection as an asset, not just a liability. Publicly facing policies should attempt to shift data protection from being merely a liability to an asset for the company, i.e. companies collect and secure a lot of data to better serve their customers.

13. Unless intended for penetration testing purposes, it is important not to take public messaging boasting your company's data security too far, thereby inviting attempted breaches. Declaring your systems to be "impenetrable" or "100% secure" only challenges hackers to test those statements, and to publicly declare victory if they prevail.

14. Reassuring consumers that your organization employs reasonable technical, administrative and physical safeguards to protect personally identifiable data is important. However, avoid the temptation to provide too much detail to the public regarding the specific safeguards that you employ. Doing so could unwittingly provide hackers a road map to your data protection systems, and, correspondingly, insight as to how to defeat them. Too much detail regarding your data protection safeguards also could make you an easier target for a lawsuit if your specific data practices change (but your public-facing policies and statements regarding those practices are not updated), or if your statements include self-imposed standards that may appeal to consumers but exceed legal requirements (*e.g.,* claims regarding "best efforts" and the like).

15. Treat your clients as stewards of their data – inform them about the way you deal with information about them. In so doing be particularly mindful of data protection laws regarding the protection of minors in the jurisdictions in which you transact business, as those laws tend to vary in each jurisdiction. Respect your clients' right to privacy as you want them to respect your ownership of your brand.

16. Strongly consider retaining legal counsel before a breach occurs and work with your counsel to set up a plan on how to deal with a breach. If a breach does occur, work with your counsel to provide customers with clear and timely communications to explain the steps that they can take to minimize harm.

VENDORS AND OTHER THIRD PARTIES

17. Take commercially reasonable steps to ensure that vendors and other third parties are contractually obligated to collector handle data employing at least the same standard of care and level of security as your company under applicable law. If you are not aware of what is or is not "commercially reasonable" in your particular industry or situation, contact other similarly situated businesses and work with your counsel to determine that the steps you take with vendors are appropriate to mitigate risk.

18. Third party vendor management should be a top security priority for companies. If not managed effectively, the use of third party vendors may expose brands to regulatory action, financial loss, litigation, and loss of reputation. To help manage these rights, brand owners should consider the following:

    a. Companies should evaluate and audit the risk and compliance profiles of all third party providers.
    b. Companies often default to completing due diligence reviews and managing only third party vendors performing IT functions, with the assumption that only traditional IT vendors pose a data breach risk.
    c. Brands should review whether your policies and technologies allow you to identify, assess, and manage all third parties for IT risk.
    d. Companies should identify all vendors or business partners that have access to IT systems as well as access to employee or customer information.

e. Companies should conduct regular due diligence reviews of their third party vendors. Managing your third parties based on the risks they pose requires having policies and procedures to control those risks throughout the life of the contract and contractual tools to manage or replace vendors.
f. Consider indemnification and minimum insurance clauses in your contracts with vendors and ensure that those clauses are meaningful in that the vendor can afford to cover the indemnified claims or has sufficient insurance coverage.

By implementing steps for identifying and managing third party access across systems, brands will be better able to mitigate the risk of data breaches associated with third party access to sensitive information.

SOCIAL MEDIA

19. A company's social media presence is one of the primary channels through which brands reach and interact with customers and the general public. In a time when a tweet or Facebook post can go viral in the blink of an eye, getting social media "right" is a pronounced challenge for brands. Observing best practices while using social media, and codifying those practices where appropriate through a well-crafted social media policy or in social media guidelines, can help brand owners protect their valuable marks by staying "on message" and reducing the likelihood of some common social media missteps. Some best practices to consider include the following:

    a. Rather than focusing your social media policy or guidelines on a set of overbroad prohibitions, consider building social media policies around a set of core social media values the brand owner wants employees and social media content to embody, e.g., truthfulness, cooperation, compliance with company policies, common sense, an awareness of the permanence of content shared via social media, and exercising good judgment in what is posted.

    b. Consider addressing proper brand usage in your social media policy as a means to guard against trademark misuse and genericide.

    c. Make clear who is, and who is not, authorized to post on behalf of your brand. Consider developing separate social media guidelines for your authorized spokespeople. Also consider legal review for new social media campaigns.

    d. Ensure that your policy identifies appropriate points of contact for media and consumer inquiries – this will help you control your messaging and may aid in damage control in the event of a social media misstep. Also consider providing a point person to address internal disputes, which may help your brand by keeping employee disputes internal and off of social media.

    e. Highlight the importance that posts made regarding company products and services (whether from the company account, the company's own social media platform, or by employees from their personal social media accounts) be truthful, since false statements by employees have led to deceptive trade practices claims.

    f. Truth in advertising applies to all media, including social media. To further avoid deceptive trade practices claims, brand owners, their employees and paid spokespersons/endorsers should follow the Federal Trade Commission's Endorsement Guides and .Com Disclosure Guide, or relevant guidelines in your jurisdiction. This is the case even of a brand's product is just mentioned in a social media post!

g. Prohibit the unlawful disclosure of customer's personal information and explicitly cite, and incorporate by reference, the company's applicable privacy policy.

h. Carefully vet prohibitions in your social media policies that could reasonably tend to chill employees' exercise of their Section 7 rights under the National Labor Relations Act. The National Labor Relations Board has become increasingly active on this front, and in addition to the burdens imposed by regulatory action, media coverage of overbroad social media policies could negatively impact a brand. There may be relevant regulations in other countries. These are just the regulations in the United States.

i. Incorporate social media policies into employee handbooks and/or issue them as stand-alone policies, depending on your company's circumstances.

j. Depending on its contents, consider including the whistleblower immunity notice language required under the Defend Trade Secrets Act of 2016. Again, there may be relevant regulations in other countries. These are just the regulations in the United States.

k. Clearly communicate social media policies in a conversational tone and in plain language. Avoid the use of complex wording or legal terms. The use of images, screen grabs, or videos should be encouraged.

l. Finally, brand owners should train their employees about the company's social media policy and be clear about expectations with respect to the avoidance of ambiguity within social media content. This can help increase employee buy-in and also explain the company's legitimate business interests underpinning the policy, including brand protection.