International Franchise Association
51st Annual Legal Symposium
May 6-8, 2018
Washington, DC

The Digital Economy: Friend or Foe to Franchising?

Leita Walker*
Faegre Baker Daniels LLP
Minneapolis, Minnesota

Jeff Norris
Choice Hotels International
Rockville, Maryland

Kathleen Ugalde
Subway Restaurants
Milford, Connecticut

* The authors extend their thanks to Faegre Baker Daniels associate Shannon Jankowski and counsel Lucie Guyot for their assistance with these materials.

Wake up any morning in any city of respectable size and—without talking to a soul or taking out your credit card—you can request a Lyft to the airport, scan a QR code to buy your coffee, check in to your hotel room with keyless entry, hit the local 24/7 gym for a self-guided workout, make sure Fido is ok at the pooch hotel by checking the live kennel cam, and then settle in for the night with commercial-free television on Netflix, while double-checking (on your connected-home app) that you shut the garage door and placing an Instacart order so you'll have milk when you get home.

To compete for customers who have come to expect such convenient, seamless experiences, franchise systems must embrace the technologies (and vendors) that make these experiences possible. In addition, franchise systems must up their marketing games. Gone are the simple days where a newspaper ad for housecleaning services was all you needed. Instead, now you might consider hiring a "mommy blogger" to write about how much easier it is to zen out when your kitchen counter tops are not only crumb free but wiped down with a chemical-free, kid-safe, essential-oil infused spray (and to put in a plug for your particular maid service brand, of course).

In short, there is never a dull moment in today's connected world for franchisors (and franchisees) intent on growing and marketing their businesses. The opportunities are real, while failure to seize them may set you back so far you can never catch up to your competitors. However, there also are legal issues that arise when companies dive into the digital, on-demand, crowd-sourced, sharing economy (how many more adjectives can we find?!). This paper explores several of those issues.

I. Protecting the brand

Most franchise systems are focused on things like making good burgers, not making a good mobile app—as well they should be. What this means, however, is that they need help from outside vendors—and they need to obtain that help while living up to the brand promise and consumer expectations. The first subsection below thus focuses on some issues to consider when negotiating a vendor contract, whether it's for the design and hosting of a new online platform, delivery of meals from local restaurants to your hotel guests, or anything in between.

The next subsection focuses on protecting the brand (and complying with the law) as your franchise system undertakes nontraditional marketing initiatives, and the final subsection offers some tips on guarding against (and dealing with) rogue franchisees.

A. Partnering with digital economy service providers

For the franchisor, technology contracts pose at least two distinct challenges. First, there's a good chance the whiz-bang technology your Chief Marketing Officer wants to implement was developed by a couple of 25-year-olds who bring their dogs to work. Not that there's anything wrong with that. But when contracting with a start-up,

there's a decent chance its owners are a lot more focused on building cool stuff than they are on making sure their company is adequately capitalized and complies with all laws and industry regulations and that it can stand behind the contract if things don't go as planned. Sure they will sign it—"As soon as possible. Just tell us where!"—but what is that contract really worth?

Second—and related to the first point—franchise systems are different than other types of businesses. Edicts from on high don't always work with skeptical franchisees. Even if a franchisor has the right under the franchise agreements to require its franchisees to adopt and implement new technology, that doesn't mean that all (or even a critical mass) of the franchisees will comply. System adoption is key to success. In addition, vendors that are not used to working with franchise systems do not understand that franchisors can't be responsible for franchisee acts/omissions and franchisors can't bind their franchisees to vendor terms and conditions, to identify just a few challenges. Your technology partner may not fully appreciate these issues or be able to easily adjust its approach.

So, pro tip No. 1 is to do your due diligence. Sophisticated companies have developed vendor assurance checklists that must be completed before the contract is signed. In the authors' experiences, two common trouble spots include the area of data privacy and security (especially PCI-DSS compliance) and vendors' ability to stand behind promises of indemnity. Does this mean you shouldn't do business with them? Not necessarily, but you should go into the contract with eyes wide open and consider whether the risk is worth the reward, as well as how you can limit your exposure (for example, by limiting the amount or nature of the data you share with the vendor).

Pro tip No. 2 is to consider a pilot program. As noted above, many technology vendors, especially the start-up variety, do not understand the nature of franchise systems and this lack of sophistication can slow down not only deal negotiation but also project implementation. Meanwhile, the franchisor needs to come to terms with how much it can require of its franchisees pursuant to the franchise agreement. And even if a franchisor can contractually impose its will upon a franchisee with regard to a particular initiative, failure to get buy-in, especially coupled with poor implementation, can result in backlash, ill will, and ultimate project failure. For this reason, pilot programs are particularly helpful in the franchise context. A new initiative can be rolled out at company-owned locations or with a couple of franchisees who are particularly game to try new things and who have a good relationship with the franchisor. After the kinks are worked out, these franchisees can be your company's ambassadors as they encourage others to embrace and adopt change.

Finally—and this is less pro tip, more table stakes—there are certain things your contracts with technology vendors should always address. They include:

- Ownership—not only of the platform, work product, or other IP the vendor develops but also of data disclosed to the vendor. Importantly, it's not enough to just say that you own the work product. The contract should contain an

explicit assignment of the work product from the vendor to the franchisor. On the data front, the default—especially as to personally identifiable information of your customers—should always be that the vendor has no claim of ownership to data disclosed to it and can use that data only for contracted-for purposes (not for its own marketing purposes).

- Representations and warranties—your vendor should represent and warrant that it owns all IP rights in the technology it is providing and that it has a right to license the technology to your company. The last thing you want is a patent suit over a QR code—just ask Wendy's.[1]
- Confidentiality and data security—in performing its services, the vendor may need access to your valuable trade secrets or your customers' personal information. Make sure the vendor is obligated to protect this information and to notify you if unauthorized access occurs. Given the inevitability of data breaches, if you're sharing personally identifiable information with your vendor—especially if you're sharing social security numbers and/or credit card or financial account numbers—include language outlining the vendor's responsibilities in the event of a suspected or actual breach. Consider adopting a standard data security addendum that can be attached to all contracts pursuant to which a vendor receives proprietary data or personally identifiable information.
- Termination—it's sad but true that some relationships take a turn for the worse. If you have to terminate an agreement with a vendor, what happens to work in progress? Will you get ownership of it? Who owns the URL through which you've built up a fan base? Do you have possession of the passwords you need? What sort of responsibilities will the vendor have to transition work to its replacement? Can the vendor go to work for a competitor?
- Indemnification and insurance—make sure the indemnification is broad enough to cover intellectual property claims arising out of the vendor's technology. And, especially if you question the vendor's financial well-being, impose an obligation that it obtain insurance and name your company as a beneficiary.

B. "News-jacking" and other cool things that scare lawyers

Social media waits for no one. Because of this, normal advertising clearance mechanisms often fall by the wayside, resulting in increased exposure—both legal and reputational. Your marketers undoubtedly will tell you that "everyone is doing it" (whatever "it" is, on any given day), but don't be lulled into a false sense of security by the "safety in numbers" argument. Ordinary consumers may not be likely to sue over a re-purposed photograph lifted from Instagram, but celebrities are another story. Regardless, your company should be deliberate about its use of social media (which

[1] Zachary Zagger, "Wendy's Can't Escape Patent Suit Over QR Code Ads," Law360 (March 5, 2015), https://www.law360.com/articles/628038/wendy-s-can-t-escape-patent-suit-over-qr-code-ads.

increasingly plays a role in contests and sweepstakes), its relationships with social influencers, and its reliance on so-called "native advertising."

Laws prohibiting false and misleading advertising are platform neutral. This means that advertising claims must be substantiated on Facebook just as they are on your website and product packaging. Further, just because your consumers are viewing your advertisements on a small screen or via a platform with a character limit does not mean you can forego a necessary disclaimer. In addition, in the age of the re-tweet and hashtag, brands should be vigilant that they are not infringing copyrights or trademarks and that they are respecting individuals' rights of publicity when using names and likenesses to promote products and services.

1. Real-time marketing

In a 2015 study, sixty-four percent of millennials stated that "they respond more positively to brand messages that are tailored to their cultural interests."[2] In an effort to generate greater cultural relevance, brands are increasingly turning to "real-time marketing." Sometimes referred to as "newsjacking," real-time marketing occurs when a brand, usually through its social media pages, attempts to interject itself or its products and services into conversations regarding current events or trends. As the name suggests, real-time marketing often follows in quick response to live occurrences, such as an awards ceremony, a big game, or a celebrity's baby announcement. By showing that the brand is engaged with topics that matter to its consumers, it hopes to garner brand awareness and loyalty. But the emphasis on speed often results in a lack of meaningful management or legal review, exposing the brand to greater risk. In addition to potential backlash from consumers, an ill-conceived tweet or Facebook post could lead to copyright, trademark, or right of publicity claims.

Celebrities have been particularly vigilant in responding to brands' use of their names or images without consent. In 2014, actress Katherine Heigl was photographed leaving a Duane Reade store, carrying Duane Reade shopping bags. The brand posted the photo on its Twitter and Facebook accounts, but did not seek the actress's consent. Heigl filed a $6 million lawsuit in the Southern District of New York, alleging unfair competition, false advertising and violation of her right of publicity. The parties ultimately settled for an undisclosed amount.

The risks aren't necessarily limited to hastily crafted social media messages. Shortly after Michael Jordan's induction into the NBA Hall of Fame in 2015, a Chicago supermarket chain published a magazine advertisement, presumably congratulating Jordan on his induction ("Congratulations Michael Jordan. You are a cut above."), and offering a coupon for steak. Jordan sued over the unauthorized use of his name and obtained an $8.9 million jury verdict, which he planned to donate to charity. A similar suit against another grocery store settled soon after.

---

[2] Michael Brenner, *Millennials Don't Want Ads. They Want Stories.,* ENTREPRENEUR, Oct. 22, 2015, https://www.entrepreneur.com/article/250243.

Arby's fared better when it grabbed the coattails of musician Pharrell Williams as part of its real-time marketing campaign during the 2014 Grammy awards. After Pharrell was spotted onstage sporting a hat similar in shape to the Arby's logo, the brand tweeted, "Hey @Pharrell, can we have our hat back? #GRAMMYs." While Pharrell responded good-naturedly ("Y'all tryna start a roast beef?"), the tweet could have exposed Arby's to the same type of right of publicity and false advertising claims as the Katherine Heigl and Michael Jordan cases.

Even outside of a legal context, real-time marketing presents increased risks of negative publicity or brand backlash, particularly if the brand fails to do its homework with respect to the trends it hopes to capitalize on. For example, after video surfaced of Baltimore Ravens running back Ray Rice assaulting his fiancé, domestic abuse survivors used the hashtag #whyIstayed to discuss the difficulties inherent in leaving an abusive relationship. Without researching why the hashtag was trending, DiGiorno's Pizza tweeted "#WhyIStayed You had pizza." The brand suffered immediate and widespread backlash and was forced to admit its lack of due diligence and—most importantly to millennials—cultural awareness: "A million apologies. Did not read what the hashtag was about before posting."

If done properly, real-time marketing can be an effective way to increase brand awareness and to connect with consumers. But it is imperative that brands establish proactive guidelines and procedures to properly vet social media messages and assess risks, even in real time.

2. Endorsements and social media promotions

Another avenue for generating awareness and customer connection is through endorsements and social media promotions. The FTC first developed its *Guides Concerning the Use of Endorsements and Testimonials in Advertising* in the 1970s, when endorsements were primarily limited to magazine ads and television commercials. The Guides apply to "any advertising message … that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser."[3] Endorsements "must reflect the honest opinions, findings, beliefs, or experience of the endorser" and "may not convey any express or implied representation that would be deceptive if made directly by the advertiser."[4]

In the late 2000s, many brands turned to popular "mommy bloggers" to help promote their products. The brand provided its products or services to the blogger free of charge in exchange for a review or an endorsement. However, not all bloggers disclosed this connection. Concerned that consumers might be misled, the FTC revised its Guides in 2009 to clarify that if there is "a connection between the endorser and the

[3] 16 C.F.R. § 255.0(b).
[4] 16 C.F.R. § 255.1(a).

seller of the advertised product that might materially affect the weight or credibility of the endorsement (i.e., the connection is not reasonably expected by the audience), such connection must be fully disclosed."[5] A material connection can be a "business or family relationship, monetary payment, or the gift of a free product."[6] In addition, both endorsers ***and advertisers*** may be liable for false statements made by the endorser and for the failure of the endorser to disclose material connections.[7]

The FTC's first foray into enforcing the revised guidelines came in 2010, when it issued a warning letter to Ann Taylor LOFT, after the store invited bloggers to a preview of its summer collection. At the preview, bloggers were provided with gift bags and the opportunity to be entered into a drawing for a gift card if they posted about the event. Although the brand displayed a sign at the event reminding bloggers of their disclosure obligations, not all bloggers who posted complied. Ultimately, the FTC elected not to pursue enforcement, as this was the first such event that Ann Taylor conducted and most bloggers who posted about the event did make the appropriate disclosures.[8] Further, the brand implemented a written policy stating that it would not provide gifts to bloggers without informing them of their obligation to disclose and agreed to monitor compliance going forward.[9]

In 2014, the FTC further clarified that its endorsement guidelines apply to any individual with a material connection to the brand, even if that individual is an otherwise ordinary consumer and the connection is entry into a contest. As part of its "Wandering Sole" contest on Pinterest, Cole Haan asked consumers to pin five images of Cole Haan shoes and five images of their favorite places to wander using the hashtag #WanderingSole. The most creative entry would win a $1,000 shopping spree. The FTC investigated, concluding that "participants' pins featuring Cole Haan products were endorsements of the Cole Haan products, and the fact that the pins were incentivized by the opportunity to win a $1000 shopping spree would not reasonably be expected by consumers who saw the pins."[10] Further, the hashtag #wanderingsole was not sufficient to communicate the material connection to consumers.[11] As it had not previously addressed whether entry into a contest was a material connection or whether a pin or other social media post would constitute an endorsement, the FTC elected not to pursue enforcement action against Cole Haan.[12] It provided some additional clarity in a subsequent FAQs document, stating that making the word "contest" or "sweepstakes" a

---

[5] 16 C.F.R. § 255.5.
[6] https://www.ftc.gov/news-events/press-releases/2017/04/ftc-staff-reminds-influencers-brands-clearly-disclose
[7] 16 C.F.R. § 255.1(d) (emphasis added).
[8] https://www.ftc.gov/sites/default/files/documents/closing_letters/anntaylor-stores-corporation/100420anntaylorclosingletter.pdf.
[9] *Id.*
[10] https://www.ftc.gov/system/files/documents/closing_letters/cole-haan-inc./140320colehaanclosingletter.pdf.
[11] *Id.*
[12] *Id.*

part of the hashtag “should be enough” to communicate the material connection, but that “sweeps” would “probably” not be sufficient, as “it is likely that many people would not understand what that means.”[13]

The Guides can also apply to a brand’s employees or to the employees of its agencies and affiliates. In 2014, the FTC charged Deutsch LA, the then-advertising agency for Sony, with misleading consumers after the agency encouraged its employees to generate “awareness and excitement” on Twitter about the Sony PlayStation Vita.[14] However, the agency did not instruct employees to disclose their material connection to Deutsch LA or the material connection between Deutsch LA and Sony.[15]

Endorsements continue to be an area of focus for the FTC, particularly as social media platforms expand and evolve. In March, 2017, “[a]fter reviewing numerous Instagram posts by celebrities, athletes, and other influencers,” the FTC sent 90 letters to marketers and social media influencers reminding them of their obligations under the Guides.[16] Noting that most individuals viewing Instagram posts on their mobile devices “typically see only the first three lines of a longer post unless they click ‘more,’” brands should ensure that disclosures appear above the “more” button.[17] Further, disclosures featuring multiple hashtags should either be avoided, or placed at the beginning of a post, rather than at the end, where consumers will likely skip over them.[18] Finally, it noted that certain short-form or indirect methods of disclosure, such as "#sp," "Thanks [Brand]," or "#partner" are not sufficiently clear, and that endorsers should use #ad or #sponsored to clarify a material connection. This also applies to celebrities and famous athletes, if “a significant portion” of his or her followers do not know that the celebrity or athlete is a paid endorser of the brand.[19] If there is any doubt or difficulty in assessing whether “a significant portion” of his or her followers would be aware of the connection, the FTC advises to err on the side of disclosure.[20]

3. Native Advertising and .Com Disclosures

Another area in which the FTC has recognized a heightened need for transparency and disclosure is what is known as “native advertising.” The FTC defines native advertising as “content that bears a similarity to the news, feature articles,

---

[13] https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking#socialmediacontests.
[14] https://www.ftc.gov/news-events/press-releases/2015/03/ftc-approves-final-orders-related-false-advertising-sony-computer.
[15] *Id.*
[16] https://www.ftc.gov/news-events/press-releases/2017/04/ftc-staff-reminds-influencers-brands-clearly-disclose.
[17] *Id.*
[18] *Id.*
[19] https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking.
[20] *Id.*

product reviews, entertainment, and other material that surrounds it online."[21] In other words, today's native advertising is yesterday's "advertorial." Often going beyond mere "similarity," native advertising is designed to be seamless and to appear that it is not a separate advertisement, but actually an organic part of the content. The Interactive Advertising Bureau describes the aspirational goals of native advertisings as "paid ads that are so cohesive with the page content, assimilated into the design, and consistent with the platform behavior that the viewer simply feels that they belong."[22] Not surprisingly, these ads typically produce higher click-through rates than traditional advertising.

The FTC has stated that it "applies the same truth-in-advertising principles" to native advertising as to all other forms of advertising."[23] In evaluating whether native advertisements are deceptive, the FTC looks to the "net impression" conveyed by the ads. [24] "[I]f they convey to consumers expressly or by implication that they're independent, impartial, or from a source other than the sponsoring advertiser—in other words, that they're something other than ads"—a "clear and prominent" disclosure is necessary to prevent deception.[25]

Responsibility for ensuring that native ads are clearly identifiable as advertising lies with the advertiser.[26]In determining whether such disclosure is needed, a brand must look to the ad's "overall appearance; the similarity of its written, spoken, or visual style or subject matter to nonadvertising content . . . ; and the degree to which it is distinguishable from other content on the publisher site."[27] The greater the similarity between the ad and the content surrounding it, the more likely the FTC will view disclosure as necessary.

When making disclosures, the FTC recommends following the guidelines identified in its *.com Disclosures Guide*.[28] Ideally, disclosures should be (a) in clear and unambiguous language; (b) as close as possible to the native ads to which they relate; (c) in a font and color that's easy to read; (d) in a shade that stands out against the background; (e) for video ads, on the screen long enough to be noticed, read, and understood; and (f) for audio disclosures, read at a cadence that's easy for consumers to follow and in words consumers will understand.[29] Although advertisers have flexibility

---

[21] https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses.
[22] https://www.iab.com/wp-content/uploads/2015/06/IAB-Native-Advertising-Playbook2.pdf.
[23] https://www.ftc.gov/tips-advice/business-center/guidance/native-advertising-guide-businesses.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*

in how to identify and disclose native ads, brands should consider the perspective of the reasonable consumer when assessing the effectiveness of the disclosure, including the size and configuration of the device on which the consumer will most likely view the ad and the words or phrases most likely to be understood by the consumer.[30] For example, the FTC views terms such as "promoted," "promoted story," "brought to you by," "sponsored by" or "presented by" as ambiguous and potentially misleading. Instead, it recommends using statements such as "ad," "advertisement," "paid advertisement," or "sponsored advertising content," and placing them as close as possible to the focal point of the ad and in front of or above the headline of the ad.[31]

The FTC's concern that disclosures meet the unique needs of "space constrained" mobile platforms extends beyond native advertising and applies to all online advertisements, endorsements and social media promotions. As detailed in its 2013 *.com Disclosures Guide*, disclosures and disclaimers must be presented "as close as possible to the triggering claim" and in a font, size, and color that is easy to read.[32] Brands should consider a variety of factors in creating and placing disclosures, such as whether a disclosure may be too small to read on a mobile device, or whether the device allows for horizontal or vertical scrolling, or both. While the Guide discourages disclaimers requiring scrolling, if doing so, brands should use text or visual cues that encourage the consumer to scroll (note: the FTC does not consider scroll bars to be "a sufficiently effective visual cue.").[33] To help brands navigate these challenges, the FTC recommends using "websites that are optimized for mobile devices or created using responsive design, which automatically detects the kind of device the consumer is using to access the site and arranges the content on the site so it makes sense for that device."[34]

The Guide permits that if a disclosure is lengthy or must be repeated frequently, brands may hyperlink to the disclosure, provided that the disclosure is not an integral part of the claim.[35] However, disclosures relating to cost or to health and safety information should not be made via hyperlink.[36] If using a hyperlink, a brand should: (a) make the link obvious; (b) label the hyperlink appropriately to convey the importance, nature, and relevance of the information it leads to; (c) use hyperlink styles consistently, so consumers know when a link is available; (d) place the hyperlink as close as possible to the relevant information it qualifies and make it noticeable; and (e) take consumers directly to the disclosure on the click-through page. In addition, brands should monitor

---

[30] *Id.*
[31] *Id.*
[32] https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*

click-through rates to assess the effectiveness of the hyperlink and make any necessary changes to ensure that consumers view the disclosure.[37]

Not surprisingly, the FTC is also unsympathetic to challenges posed by the character limits or format of any particular social media platform: "If a disclosure is necessary to prevent an advertisement from being deceptive [or] unfair … and if it is not possible to make the disclosure clear and conspicuous, then either the claim should be modified or the ad should not be disseminated. Moreover, if a particular platform does not provide an opportunity to make clear and conspicuous disclosure, it should not be used to disseminate advertisements that require such disclosures."[38] The bottom line for the FTC: if you can't fit all of your copy and required disclosures in 140 (or 280) characters, then don't post the ad on Twitter. #harsh.

C. Guarding against the rogue franchisee

Finally, although legal, successful attempts to exploit the digital economy require advance planning, thoughtful strategy, and attorney input, the technology itself is readily available—which raises the specter of the rogue employee/franchisee. They mean well. They are thinking creatively and trying to grow their business and often they "go rogue" because they feel like the franchisor isn't keeping up with consumer expectations/market demand. But before you know it, those business cards collected in the fishbowl drawing for a dozen bagels have been loaded into a database, text messages are going out, and you're having to study up on the Telephone Consumer Protection Act. Major bummer.

The availability of relatively cheap technology coupled with franchisees who are more entrepreneurial than they are legally savvy means the franchisor must be especially vigilant. At the same time, it cannot be too heavy-handed—the goal is to walk the line of allowing franchisees to conduct their business while stll protecting the brand and ensuring that franchisees follow all applicable laws and system standards.

Franchisor policies can help mitigate these issues and create a cohesive brand message. Thus, consider what controls your company includes in its franchise agreement and/or operations manual (and think about whether those controls are manageable and/or whether they unnecessarily create liability risks for the franchisor).

Some franchisors, for example, simply say that the franchisee must follow its social media policy (if you take this approach, make sure yours is sufficiently robust!), while others retain the right to approve all social media posts. The latter may not be workable, depending on the size of your system and the franchisor's resources. Likewise, some systems prohibit franchisees from creating a website or social media account without approval, while others just require franchisees to disclose their passwords so that the franchisor can commandeer the website/account to take

---

[37] *Id.*
[38] *Id.*

corrective action and/or operate the account after termination of the franchise agreement. (Indeed, this should be a minimum standard in your franchise agreement.) Attached as Appendix A is a sample social media policy.

In addition, consider creating tools to help your franchisees help themselves. For example, if you provide a website template to them, they are less likely to create one on their own that flies in the face of the message the brand is trying to send. Companies have also found it useful to offer educational materials and training to franchisees on a variety of topics and to create qualified vendor programs so that franchisees can choose from a pool of approved vendors, which gives them a feeling of control without creating unacceptable levels of risk for the system.

II. Leveraging Big Data while complying with the law

You want a pizza, but don't want to deal with phone call? Understandable. How many of us have called during the nightly rush, only to be put on hold, and then had to shout our credit card number so the teenager on the other end could hear it over the clattering dishes. And then the pizza arrives and it was supposed to be half cheese but it's not and now the 4-year-old is having an absolute meltdown. The struggle is real.

But in 2018? No problem. Open up the franchisor-owned mobile app—your credit card number is already uploaded—and pick your toppings and delivery time. Your order will zing its way through a server in Nebraska before appearing on a screen at the pizza place just down the street. Really, even a monkey can take it from here.

And now, the franchisor has a direct line of communication with you. So they will tally your loyalty points and send you an email reminder that you get $5 off next time. Life is good.

The example above illustrates one of the major impacts of the digital economy: centralization. Customers are now interacting directly with the franchisor, and the franchisor is then dribbling out to the local franchisee whatever it needs to provide the product/service. Meanwhile, the franchisor has now established a direct line of communication with the customer for purposes of marketing and other communications.

There's a lot of upside to this for the consumer and the franchisor, but it can create tensions with franchisees. In the hospitality industry, for example, a franchisee might also own a mom-and-pop restaurant and would resent it if the franchisor began emailing guests coupons to the local Olive Garden. Likewise, in the fast-food industry, franchisees may be concerned about how an app will ensure that customer orders are sent to stores in a consistent, non-biased way (i.e., is the correct store showing up when the consumer searches for nearby locations?). The key, the authors have found, is to ensure reliable, equitable systems are in place and then to communicate clearly and transparently with franchisees to establish a level of trust.

On the flip side, sometimes the franchisee is driving centralization. They often look to the franchisor to develop the tools necessary to drive sales (such as remote ordering and loyalty programs). Large franchisors—especially those that are multi-national—can struggle to make these tools fast enough to meet franchisee expectations given the various backend IT systems they rely upon and the legal issues they raise across various jurisdictions. Likewise, though systems and jurisdictional issues are often less complex for the start-up franchisor, it also may not have the resources to keep up with the technology demands of consumers. Seeking advisory input from franchisees and engaging franchisees (through a pilot program or a focus group) as a resource in the process of identifying and researching available technologies and deciding on the most suitable technology platform may help the resource-strained franchisor as well as with the system adoption of the technology.

And once the centralized technology tools are rolled out, franchisors may find themselves in possession of personally identifiable information about customers they don't need—and don't want. Chief Marketing Officers will tell you there's no such thing as too much data—"Never delete anything!" But Chief Legal Officers will tell you, like Spiderman, that "With great power comes great responsibility." While there are many benefits to centralizing data and subsequently exploiting it, the liabilities and risk to the company also increase.

To discuss all of those liabilities and risks, dear reader, would push your patience with this paper past the breaking point. We are obviously very funny with our cheeky comments, but not that funny.

So let us focus on three: clarity with your franchisees and vendors, transparency with your consumers, and—for the multinationals—compliance with the European Union's General Data Protection Regulation.

A. Know where you stand with your franchisees and vendors

As interactions with consumers become more centralized, and as franchisors increasingly rely on vendor technology to manage those interactions, contractual clarity is essential. Your franchise agreement should explicitly state that, as between the franchisor and franchisee, the franchisor owns all customer data. It should spell out what the franchisee can do with that data during the term of the franchise agreement and after the franchise agreement terminates.

Likewise, as discussed above, before sharing customers' personally identifiable information with vendors, the vendor should be bound to protect that data and also to use it only for contracted-for purposes. The contract should also state whose privacy policy will be posted on any vendor-created platform. Vendors often think it should be theirs, though this rarely makes sense from a consumer perspective. The consumer, after all, doesn't have a relationship with the vendor. They have a relationship with you, the franchisor, and if they have a problem with how their information is being used, it's you they are going to contact.

B. Give your customers accurate disclosures and meaningful choices

If clarity is the goal with franchisees and vendors, *transparency* is the goal with consumers. In the United States, there are relatively few restrictions on what companies can do with consumer's personally identifiable information. Instead, the way companies get in trouble is by using consumer data in a way they promised they would not.

The Federal Trade Commission is the chief privacy regulator in the United States, and it exercises its authority pursuant to Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices.[39] Historically, the FTC brought most investigations under the deceptive prong of the act. For example, in 2011 Facebook settled FTC charges alleging Facebook deceived consumers by telling them they could keep their information on Facebook private and then repeatedly allowing it to be shared with the public.[40] The FTC has repeatedly made clear that it will interpret privacy policies very literally and that they must be absolutely true. Thus, for example, more than one company has had an M&A deal derailed by promises in the seller's website privacy policy that "We will never sell your data."[41] Attached as Appendix B is a sample website privacy policy.

In recent years, the FTC has also begun to bring privacy and data security related actions pursuant to the unfair prong of the act, most notably against Wyndham hotels. That enforcement action arose out of three data breaches in 2008–2009 in which hackers stole personal and financial information of hundreds of thousands of Wyndham guests, resulting in fraudulent charges of over $10 million. Based on a belief that the security measures Wyndham had in place to prevent and detect a breach were woefully inadequate, the FTC brought unfair practices action against it. Wyndham challenged the FTC's expansive view of its power but in 2015 the Third Circuit held that the FTC could, indeed, pursue an enforcement action.[42] After setting out the history behind the FTC Act, the Third Circuit held that it "requires [1] substantial injury that [2] is not reasonably avoidable by consumers and that [3] is not outweighed by the benefits to consumers or competition" but "acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive."[43]

---

[39] 15 U.S.C. § 45(a).

[40] Press Release, "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises," FTC.com (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[41] *See, e.g.*, Press Release, "FTC Requests Bankruptcy Court Take Steps to Protect RadioShack Consumers' Personal Information," FTC.com (May 18, 2015), https://www.ftc.gov/news-events/press-releases/2015/05/ftc-requests-bankruptcy-court-take-steps-protect-radioshack.

[42] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3rd Cir. 2015).

[43] *Id*. at 244 (citing 15 U.S.C. § 45(n)).

In so holding, the Third Circuit rejected Wyndham's argument that it lacked notice of what specific cybersecurity practices were necessary to avoid liability.[44] While recognizing that the language of § 45(n) of the FTC Act was "far from precise" and could result in some "borderline cases," the court stated that the relevant inquiry was a "cost-benefit analysis" that required consideration of a number of factors, "including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity."[45] The Court held that Wyndham's fair notice challenge fell short, given that the FTC's complaint did not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords.[46] Instead, the FTC's complaint was based on the absence of any firewall at critical network points, Wyndham's failure to restrict specific IP addresses, its lack of any encryption for certain customer files, and its failure to require some users to change their default or factory-setting passwords.[47] The Court found that given that Wyndham was hacked three times, "it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis."[48] In addition, the Court's decision was reinforced by language regarding sound data security plans from the FTC Guidebook, as well as published FTC complaints and consent decrees from administrative cases that provided Wyndham notice of the FTC's expectations with regard to cybersecurity.[49]

C. Comply with the EU's General Data Protection Regulation

As if this weren't complicated enough, companies who operate overseas must also consider the data protection laws in the jurisdictions where they have employees or franchisees—and the big one on everyone's mind right now is the European Union's General Data Protection Regulation ("GDPR"). Although a deep dive into the GDPR is beyond the scope of these materials, a brief overview is in order.

The law will go into effect on May 25, 2018, and will usher in radical changes to EU data privacy laws—and greatly expand their territorial reach. The GDPR will impact U.S. businesses regardless of whether they have a corporate presence in the EU or use EU-based assets to process data (which are the current tests under the 1995 EU Data Protection Directive). If a U.S. franchisor or its franchisees offer goods or services to EU-based customers, or monitors their behavior—for example, through data analytics—they will potentially be within the scope of the GDPR.

The extra-territorial reach of the GDPR means that in practice, many businesses operating internationally will need to adopt European data privacy standards, which are

---

[44] *Id*. at 255.
[45] *Id*.
[46] *Id*. at 256.
[47] *Id*.
[48] *Id*.
[49] *Id*. at 256-57.

likely to become the default global standards. The increased sanctions under the GDPR (up to a headline-grabbing four percent of global revenue), together with general public expectations on data privacy, mean that compliance with data privacy laws cannot be treated as a minor regulatory issue. The level of fines and other penalties puts data privacy at the same level as antitrust or anti-bribery and corruption compliance on the corporate compliance agenda. This will require board-level awareness and leadership, and the combined input from a range of professionals including, legal, IT, finance, procurement and vendor management and HR.

In particular, the GDPR:

- Introduces new rights that may require changes to:
  - Privacy policies
  - Internal procedures
  - Technology platforms
  - Vendor agreements

- Introduces new obligations covering:
  - Requirements for consent
  - Data breach notification
  - Appointment of third party data processors
  - Appointment of representatives

- Requires new processes including:
  - Privacy Impact Assessments
  - Internal record-keeping/audit trail
  - Privacy by design and default
  - Implementing robust data security measures (e.g., pseudonymization and anonymization)

- Potentially requires hiring new personnel (or re-assignment of existing personnel) as a Data Protection Officer

- Has significant penalties for non-compliance (up to the greater of €20,000,000 or 4 percent of worldwide annual turnover for the most serious breaches)

The GDPR is intended to provide much greater harmonization than at present, although some differences will remain. Some areas, notably personal data relating to employees, remain subject to significant national variances. The United Kingdom will adopt the GDPR, despite its planned withdrawal from the EU in 2019. This reflects the fact that a high level of protection for personal data is expected in many modern economies and the global trend towards higher levels of protection. In particular, it provides a firmer basis for the U.K. to be recognized by the EU as offering an adequate level of protection for international transfers of personal data.

Often franchisees based in the EU are not equipped to handle GDPR compliance. Although there are many reasons, both financial and legal, that the US-based franchisor may not want to take on the compliance burden, most companies are at least providing high-level guidance to their franchisees about what GDPR is and advising them to consult with local counsel.

III. Mobile marketing and the ongoing threat of the Telephone Consumer Protection Act

A. Background on TCPA

The Telephone Consumer Protection Act (TCPA) was enacted in 1991 as a response to an increasing number of consumer complaints regarding telemarketing calls and communications.[50] However, its reach is not limited to telemarketing. Instead, it imposes restrictions any time a company uses an "automatic telephone dialing system" to call a cell phone and any time a company uses an "artificial or prerecorded voice" to deliver a message to a cell phone—regardless whether the call has a marketing-related purpose. It also imposes restrictions any time a company uses an "artificial or prerecorded voice" to deliver a marketing-related message to a residential line. Notably, the TCPA does not apply to business lines, but it does apply to both cell phones and residential land lines. It also applies to text messages, which courts have interpreted as falling within the TCPA's definition of a "call."[51]

The term "automatic telephone dialing system" ("ATDS") is a defined term in the TCPA that means "equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers.[52] The Federal Communications Commission (FCC), which issues rules under the TCPA, has in recent years taken a very broad interpretation of the statutory definition. As set forth in a 2015 omnibus order:

> We agree with commenters who argue that the TCPA's use of "capacity" does not exempt equipment that lacks the "present ability" to dial randomly or sequentially. We agree that Congress intended a broad definition of autodialer, and that the Commission has already twice addressed the issue in 2003 and 2008, stating that autodialers need only have the "capacity" to dial random and sequential numbers, rather than the "present ability" to do so. Hence, any equipment that has the requisite "capacity" is an autodialer and is therefore subject to the TCPA.
>
> … In other words, the capacity of an autodialer is not limited to its current configuration but also includes its potential functionalities.[53]

---

[50] 47 U.S.C. § 227

[51] *See, e.g.*, *Satterfield v. Simon & Schuster, Inc.*, 569 F.3d. 946, 949 (9th Cir. 2009).

[52] 47 U.S.C. § 227(a)(1).

[53] 2015 Declaratory Ruling, 30 FCC Rcd. at 7974, ¶¶ 15–16.

In fact, in language that would be laughable but for the repercussions of violating the TCPA, the FTC acknowledged that although "there are outer limits to the capacity of equipment to be an autodialer" the only technology it was willing to identify as clearly falling outside the definition was a *rotary phone*:

> [T]he outer contours of the definition of "autodialer" do not extend to every piece of malleable and modifiable dialing equipment that conceivably could be considered to have some capacity, however small, to store and dial telephone numbers …. Thus, for example, it might be theoretically possible to modify a rotary-dial phone to such an extreme that it would satisfy the definition of "autodialer," but such a possibility is too attenuated for us to find that a rotary-dial phone has the requisite "capacity" and therefore is an autodialer.[54]

As discussed in further detail in the next section, the Federal Circuit recently rejected the FCC's broad view, but the ramifications of that decision have yet to play out. Thus, when in doubt, the safe path is to assume the technology used to make calls or send text messages qualifies as an ATDS.

The TCPA does not actually prohibit calls to cell phones made with an autodialer or that use an artificial/prerecorded voice. Instead, it requires that companies obtain prior express consent before making such calls. When the call to a cell phone "includes or introduces an advertisement or constitutes telemarketing," consent must also be in writing.[55] Likewise, prior express written consent must be obtained before calling a residential line using an artificial or prerecorded message that introduces an advertisement or constitutes telemarketing.[56]

Rules promulgated under the TCPA define "advertisement" as "any material advertising the commercial availability or quality of any property, goods, or services."[57] They define "telemarketing" as "the initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services, which is transmitted to any person."[58]

---

[54] *Id.* at 7975, ¶ 18.
[55] 47 C.F.R. § 64.1200(a)(2).
[56] An exception to the consent requirements for both cell phones and residential lines exists when the call delivers a "health care" message made by, or on behalf of, a "covered entity" or its "business associate," as those terms are defined in the HIPAA Privacy Rule, 45 C.F.R. 160.103. Because Coloplast is not a covered entity or business associate and CARE Program calls are not made on behalf of a covered entity, we do not believe that exception applies here. 47 C.F.R. § 64.1200(a)(3).
[57] 47 C.F.R. § 64.1200(f)(1).
[58] *Id.* § 64.1200(f)(12).

The FCC has provided further guidance on the meaning of these terms. In a 2012 order it stated that "if the call, notwithstanding its free offer or other information, is intended to offer property, goods, or services for sale either during the call, or in the future, that call is an advertisement." The FCC also stated in that order that analysis of telephone solicitation turns "not on the caller's characterization of the call, but on the purpose of the message." And in a prior 2003 order, the FCC stated:

> The TCPA's definition does not require a sale to be made during the call in order for the message to be considered an advertisement. Offers for free goods or services that are part of an overall marketing campaign to sell property, goods, or services constitute "advertising the commercial availability or quality of any property, goods, or services." Therefore, the Commission finds that prerecorded messages containing free offers and information about goods and services that are commercially available are prohibited to residential telephone subscribers, if not otherwise exempted.

"Prior express written consent" is defined in a rule promulgated under the TCPA as:

> [A]n agreement, in writing, bearing the signature of the person called that clearly authorizes the seller to deliver or cause to be delivered to the person called advertisements or telemarketing messages using an automatic telephone dialing system or an artificial or prerecorded voice, and the telephone number to which the signatory authorizes such advertisements or telemarketing messages to be delivered.
>
> > (i) The written agreement shall include a clear and conspicuous disclosure informing the person signing that:
> >
> > > (A) By executing the agreement, such person authorizes the seller to deliver or cause to be delivered to the signatory telemarketing calls using an automatic telephone dialing system or an artificial or prerecorded voice; and
> > >
> > > (B) The person is not required to sign the agreement (directly or indirectly), or agree to enter into such an agreement as a condition of purchasing any property, goods, or services.
> >
> > (ii) The term "signature" shall include an electronic or digital form of signature, to the extent that such form of signature is recognized as a valid signature under applicable federal law or state contract law.[59]

[59] 47 C.F.R. § 64.1200 (f)(8).

In other words, the called party has to be informed (1) that she is consenting to receive calls made using an automatic telephone dialing system or an artificial or prerecorded voice and (2) that her consent is not necessary to do business with the company. The called party then has to consent in writing.

The TCPA provides a private right of action and statutory damages of $500 per call or text (or up to $1,500 per call or text where the violation is willful).[60] When a call center is making calls all day, every day, the number of calls quickly escalates and this, along with TCPA's statutory damage provision, has led to a perfect storm of class action litigation. Defendants named in these lawsuits face potential exposure that runs into the billions of dollars, and thus the cases almost always settle (often for seven figures or more). In our experience, insurance rarely covers the costs of defense or the settlement amount. In fact, litigation risks resulting from the TCPA have caused major companies to stop autodialing altogether and to instead manually dial all calls, even though this will incur additional operational costs.

B. The evolving definition of ATDS and the *ACA* Decision

As noted above, the D.C. Circuit recently issued a decision rejecting certain FCC interpretations of the TCPA. In 2015, a coalition of businesses and other organizations, including ACA International, the U. S. Chamber of Commerce, the Consumer Bankers Association, Sirius XM Radio, and Rite Aid, among others, petitioned the court to review the reasonableness of certain aspects of the FCC's omnibus order. On March 16, 2018, the court issued its decision, unanimously rejecting the FCC's construction of "capacity" with respect to autodialers.[61] The court concluded that under the current construction—which encompasses both a device's present abilities and its potential functionalities—"ordinary calls from any conventional smartphone" could be subject to the provisions of the TCPA, creating "an unreasonably expansive interpretation of the statute."[62]

In addition, the court vacated the FCC's position that, with the exception of a one-call safe harbor, calls made to a number assigned to a consenting party but later reassigned to a nonconsenting party are a violation of the TCPA, regardless of whether the caller is aware of the reassignment.[63] Finding that the agency "gave no explanation of why reasonable-reliance considerations would support limiting the safe harbor to just one call or message," the court set aside the approach as "arbitrary and capricious."[64]

The court did uphold two pieces of the 2015 order, including the FCC's conclusion "that 'a called party may revoke consent at any time and through any reasonable means'—orally or in writing—'that clearly expresses a desire not to receive

---

[60] 47 U.S. Code § 227(c)(5).
[61] *ACA Int'l v. Fed. Commc'ns Comm'n*, 885 F.3d 687, 692 (D.C. Cir. 2018).
[62] *Id.*
[63] *Id.*
[64] *Id.* at 707.

further messages.'"[65] It also upheld the FCC's framing of the exigent healthcare exemption.[66]

While many initially celebrated the decision, the court's only charge was to evaluate the reasonableness of the 2015 order, and it therefore did not provide an alternative definition or approach for either of the issues on which it rejected that order. What constitutes an autodialer and whether (or when) liability attaches with respect to reassigned numbers thus remain open questions under the TCPA. At least until the FCC issues a new, clarifying order, companies are thus advised to take a broad view of the sort of equipment that constitutes an ATDS and to continue to guard against the risks posed by reassigned numbers.

[65] *Id*. at 709 (quoting 2015 Declaratory Ruling, 30 FCC Rcd. at 7989-90 ¶ 47, 7996 ¶ 63).
[66] *Id.* at 710–14.

APPENDIX A

SAMPLE* SOCIAL MEDIA POLICY

Purpose

The Company recognizes that some Company employees may participate in online electronic communities such as Facebook, LinkedIn, Twitter, or other forms of online "social media." Without discouraging employees from engaging in social media, the Company seeks to assure that employee use or misuse of this powerful communication tool does not directly or indirectly interfere with an employee's job performance, the performance of others, the work environment or the legitimate business interests of the Company. Accordingly, the Company has established this policy regarding employee participation in social media.

Scope

This policy applies to all employees of the Company. Employees who engage in the use of online social media are expected to adhere to all applicable Company policies. This Company policy is in addition to, and not in place of, other Company policies. This policy is not intended to restrict the flow of useful and appropriate information or legally protected communications.

Enforcement

Violation of Company policies while using online social media, even outside of work, may result in disciplinary action, up to and including termination of employment. The Company may also impose disciplinary action, up to and including termination of employment, if any material posted online causes the Company to lose confidence in the employee's judgment or fitness for his or her job. However, the Company will not take adverse action against employees solely because they use social media for personal interests and affiliations or other lawful purposes during non-working time.

The Company may monitor what employees openly publish or post on the Internet or what employees otherwise make accessible to the Company, directly or indirectly, to the fullest extent permitted by law. Activity on Company computers is not private, and Internet activity on personal computers may be public and therefore accessible to the Company, unless the user adopts passwords, privacy settings or other protections precluding legitimate access by the Company.

General Provisions

Employees must follow these rules whenever using online social media:

1. Do Not Use or Disclose Confidential or Proprietary Information

The Company relies on its employees to protect its confidential and proprietary information, such as customer information, trade secrets, financial information, development activities, marketing and sales practices, manufacturing processes and strategic business plans. Accordingly, when using

* This sample is provided for general information purposes only. You should not use this sample document without first seeking legal advice. The provision of this sample document does not constitute legal advice and no lawyer-client, advisory, fiduciary or other relationship is created by virtue of this sample being provided.

social media employees may not disclose confidential or proprietary information of the Company, or any information that would compromise security at the Company.

Employees should not post work-related photographs of other employees or other business partners of the Company without their prior consent. Employees should not post photographs of non-public Company facilities, property or equipment without authorization.

Employees must not violate the confidentiality policies of the Company or the terms of any confidentiality agreement between the employee and the Company.

2. Do Not Misuse Company Time and Resources

Working time is for work. Employees who engage in the personal use of online social media are expected to do so during non-working time. Special rules may apply to any team member who requires access to online social networks for the purpose of performing his or her job responsibilities for the Company, such as marketing, recruiting, or monitoring team member compliance with this policy.

The Company's computer systems, including its e-mail and Internet connection, are the property of the Company and intended for business use. Employees must comply with Company policy regarding Internet and e-mail usage at all times.

3. Do Not Make Unauthorized Statements on Behalf of the Company

To assist the Company to maintain a consistent public persona, only authorized employees may make statements on behalf of the Company. If employees electronically publish anything that discloses their association with the Company, whether or not on Company-sponsored platforms, they must never write or post anything that leaves readers with the impression they are speaking on behalf of the Company, unless they are authorized to do so. Without such authorization, employees must make clear that their postings and views are theirs alone and not those of the Company.

4. Be Professional and Respectful

Employees must comply with all other Company policies, including without limitation the Company's anti-discrimination and non-harassment policies, regarding respectful interactions in the workplace when using social media. For example, employees may not harass or discriminate against another employee or other business contact of the Company through social media use in the same way they are prohibited from engaging in such behavior in person or through other methods of communication.

No employee may unilaterally publish or post any statement (including a photograph or other visual image) about the Company that damages the reputation of the Company if (a) the employee knows the statement is false or reasonably should have known the statement was false; or (b) the employee is acting maliciously and without any legitimate purpose protected by law.

No employee may publish or post any offensive or unprofessional material that serves no legitimate purpose protected by law and reflects poorly on the Company.

No employee may publish or post anything that a client or another Company employee would reasonably consider to be hostile, threatening, or intimidating and in violation of Company policies.

The Company's Social Media Policy does not, in any manner, prohibit employees from discussing wages, benefits, and other terms and conditions of employment or workplace matters of mutual concern that are protected by the National Labor Relations Act.

If you are uncertain about whether your use of online social media complies with this policy, you should contact your manager or Human Resources.

APPENDIX B

SAMPLE[*] ONLINE PRIVACY POLICY

Choice Hotels International, Inc.
Global Privacy & Security Policy

Choice Hotels International, Inc. and its subsidiaries ("Choice", "we" or "us") are committed to providing you with an efficient and customized Internet experience. This online Privacy and Security Policy describes the information we collect through our websites and personal devices, how we use that information, and how we protect your personally identifiable information. This policy also sets forth our practices for obtaining personal information from other sources, such as written or verbal communications or information collected at a hotel.

This policy was last modified on March 1, 2018.

GLOBAL PRIVACY & SECURITY POLICY

Hotels franchised under Choice's brand ("Franchised Hotels") are independently owned and operated. Your personal information collected or maintained directly by the Franchised Hotels is not subject to this policy, unless such information has been shared with us, in which case the policy only covers Choice's collection, use, and maintenance of your personal information. If you book a reservation directly with a hotel and that hotel utilizes our proprietary property management system, your personal information related to that reservation will be transmitted to and processed by Choice. We do not control the collection, use, or access of your information by the Franchised Hotels and their staff. The Franchised Hotel is the merchant who collects and processes credit card information and receives payment for your stay. The Franchised Hotels are subject to the merchant rules of the credit card processors they select, which establish credit card security rules and procedures.

By submitting your personal information to us, you agree to the transfer to and processing of your personal information in the United States in accordance with the terms of this Policy.

---

[*] This sample policy does not reflect the requirements of the EU's General Data Protection Regulation. Moreover, it is provided for general information purposes only. You should not use this sample document without first seeking legal advice. The provision of this sample document does not constitute legal advice and no lawyer-client, advisory, fiduciary or other relationship is created by virtue of this sample being provided.

What information do we collect?

Our websites and mobile applications may receive and store information based on your browser settings, which may include your browser type and operating system, the various Choice web pages you view, Internet Protocol addresses, unique device identifiers, and sites visited before viewing our websites. When applicable, we may compensate other websites that include links to our websites. If you have enabled the location settings on your device while our mobile app is open, we may also receive your precise geo-location information. If you have location settings turned off while our mobile app is open, we may receive your general location (country, state, city) information.

When you use our reservation system, call our toll-free reservation telephone number, become a Choice Privileges® member, create an online account, elect to receive offers, or purchase a gift card, we collect personally identifiable information and other information that you supply, such as your name, address, telephone number, e-mail address, room preference, credit card details, day and month of your birth date, and Choice Privileges number. We may also ask for additional information such as an association number (e.g., AAA), corporate account number or group booking number.

If you choose to earn airline miles or other third-party loyalty program points for your award-eligible stay at a Franchised Hotel, we will ask you to provide us your membership number for such loyalty program.

Choice may occasionally conduct sweepstakes and contests that offer you the opportunity to win prizes. As part of entering a sweepstakes, certain personally identifiable information such as name, mailing address, e-mail address and Choice Privileges number may be required.

When you request information regarding franchise opportunities from our informational website http://www.choicehotelsfranchise.com or elsewhere, we may collect information such as your contact details, your hotel ownership or development experience, the brand you are interested in, and the anticipated investment amount.

Children's Privacy: Our websites are not intended for children and we do not knowingly solicit or collect personal information for persons under the age of 18.

How do we use the information we collect?

We do not sell, trade, rent, or release your personal information to anyone outside our company, contractors, affiliates or Franchised Hotels, other than in compliance with this privacy and security policy. We and our affiliates use the personal information to administer our business activities, provide customer service, personalize your digital experience, contact you concerning your stay with a Franchised Hotel, and make other products and services available to you. We chare your information with our Franchised Hotels, credit card issuers, and other companies where necessary to complete your transaction. We may also use your information to send you promotional communications by mail or e-mail, or through our mobile apps, or share your information with our business partners.

Reservations

We maintain a centralized reservations system that retains your personally identifiable information when you make a reservation for a Franchised Hotel via our worldwide accessible websites, mobile apps, our call centers, the Franchised Hotels, and third-party travel agents and travel websites that connect to our reservation system. The personal information collected in the reservation system is needed to secure and process your reservation. Your personally identifiable information (including credit card number) will be processed primarily in the United States to complete your transaction and to facilitate the making of future reservations. Only that personal information which is reasonably required to facilitate your reservations is collected and shared between Choice and the Franchised Hotels.

We will use your e-mail address to send a confirmation and, if necessary, might use the other information to contact you regarding your reservation. We may also use your e-mail address to:

- send you travel-related messages, stay details, and provide other information about the area and the Franchised Hotel;
- notify you about special offers and promotions; and
- send you periodic satisfaction or market research surveys.

Such information may also be sent to you through our mobile apps, if you elect to receive notifications and alerts.

Marketing, Sweepstakes & Contests

We may use your personal information to send you via e-mail, telephone, mobile app or postal mail promotions, surveys, third party offers, sweepstakes and contests.

Choice Privileges Members

If you are a Choice Privileges member, we will use your personal information to perform certain administrative tasks necessary for the administration and operation of the program such as: (1) allowing you to earn Choice Privileges points for point-eligible stays at various Franchised Hotels; and (2) redeem Choice Privileges points for free nights and other rewards offered by the program.

We may also use your personal information to send you via e-mail, telephone, mobile app or postal mail program details, account summaries, satisfaction surveys, promotions, third party offers, sweepstakes and contests. We may also contact you about applying for the Choice Privileges Visa® card issued by Barclays Bank Delaware (Barclay card member FDIC, pursuant to license from Visa USA Inc.).

Choice Privileges members' personal information may be collected through Choice's websites, mobile applications, Choice's call centers, paper applications, or may be passed on to Choice by Franchised Hotels. Choice may transfer personal information to Franchised Hotels as a part of

administering the Choice Privileges program as outlined above. Choice processes Choice Privileges members' personal information primarily in the United States.

E-Folio

If you participate in the electronic billing e-folio program, your hotel bill will be sent to you over the Internet in an unsecure (unencrypted) manner – by email or through our mobile applications, depending on your preference and selection - and could be subject to interception by third parties. If you use a corporate credit card, billing information and the details of your hotel stay will be shared with the credit card provider who, in turn, will provide it to your employer.

Other Uses of Personal Information

To serve you better, Choice may combine information you give us online, at Franchised Hotels, through the mail, or in any other way. Choice may also combine that information with publicly available information and information Choice receives from others or cross-references. Choice uses that combined information for the purposes described in this privacy statement.

To the extent required or permitted by law, we may collect, use and disclose personal information in connection with security-related or law enforcement investigations or in the course of cooperating with authorities or complying with legal requirements. We may also use your information as permitted by law to perform credit checks, report or collect debts owed, or protect the rights or property of Choice, our employees, our Franchised Hotels, our customers, this site, or its users.

Do you share my personal information with third parties?

As noted above under "Reservations," Choice will need to transfer your personal information to Franchised Hotels to secure your reservation or in connection with awarding or redeeming Choice Privileges points. Please note that some hotels may be in countries other than your country of residence and may not provide an equivalent level of data protection.

Choice distributes personal information about guests and Choice Privileges members to third party service providers such as web analytics companies, market researchers and fulfillment houses. We also use such third parties to: (i) conduct data processing for Choice, (ii) engages in e-mail and direct mail communications on behalf of Choice, (iii) administer sweepstakes and contests, (iv) administer guest surveys, (v) compile information for us about the type and frequency of guest stays and the use of the Choice Privileges program by members, and (vi) compile information for us about the use of Choice's websites and mobile apps. These parties are contractually prohibited from using personally identifiable information for any purpose other than the purpose that Choice specifies.

Choice may also distribute personal information to airline and other companies upon request of guests, in order to allow guests to: (i) earn frequent customer miles/points with such airline and other companies for stays at hotels, or (ii) redeem Choice Privileges points for goods and services of such airline and other companies.

Choice may partner with other companies to provide co-sponsored or co-branded promotions, sweepstakes, contests, products and services and may share your information with these companies.

As available in specified regions, if you choose to apply for a Choice Privileges Visa card, you will be linked from Choice's website to Barclays Bank Delaware's website and will be required to enter certain personally identifiable information as part of the credit application process. Please refer to Barclays Bank Delaware's privacy statement posted on their website to understand how the information you supply will be used.

Although unlikely, in certain instances, Choice may disclose your personally identifiable information when Choice has reason to believe that it is necessary to identify, contact or bring legal action against persons or entities who may be causing injury to you, to Choice or to others. Choice may also disclose your personally identifiable information when Choice believes the law requires it.

We may disclose your personal information to a third party in the event of any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings).

Special Notification to California Residents: If you reside in California and have provided Choice your personally identifiable information, you may request a list from us of third parties with whom we shared your personally identifiable information for their own direct marketing purposes during the preceding calendar year. Such requests must be submitted to us at: Privacy@choicehotels.com or Choice Hotels International, Attention: Privacy Officer, 6811 E. Mayo Blvd., Suite 100, Phoenix, Arizona 85054. This request may be made no more than once per calendar year.

How do I opt-out of marketing communications or otherwise change my privacy preferences?

We respect the right of each visitor to control how his or her personal information is used. If you do not want us to provide your information to our business partners, or if you do not wish to receive promotional communications from us or our affiliates concerning special offers, discounts, airline bonuses, or contests, select one of the following options to provide us with your privacy preferences:

Click here if you have an Online Account and edit your privacy preferences within your account.

- OR -

If you do not have an online account and do not wish to create one, click here to provide us with your privacy preferences.

- OR -

Use the "Unsubscribe" function in the e-mail you received from us.

You can also e-mail us at Privacy@choicehotels.com or write to Choice Hotels International, Attention: Privacy Officer, 6811 E. Mayo Blvd., Suite 100, Phoenix, Arizona 85054. Please include your name, address, e-mail address and Choice Privileges number (if applicable) and clearly state the nature of your request.

Choice makes every reasonable effort to maintain the accuracy of personal information. If you become aware that information Choice maintains about you is incorrect or if you would like to update your information, please contact us as indicated above.

How do you store and secure my personal information?

Our reservation system and other databases are maintained in the United States; therefore, your personal information will be collected (or transferred) and maintained in the United States. Once your information reaches us, we treat it as confidential and protect it through a variety of generally accepted industry standards.

When you provide us with information through this site, such as your name, address, phone number, credit card information and room preference, your information will be encrypted using a Transport Layer Security or a Secure Sockets Layer connection. You can tell if your information is encrypted by looking for the locked padlock icon on the lower right-hand or left-hand corner of your screen and a change in the site address from "http" to "https."

Do you use “cookies” and similar technologies?

Choice’s Websites, mobile applications and e-mails may use “cookies” and other computer code processes. These are small amounts of computer code that interact with your computer, mobile device, browser or e-mail. The types of cookies Choice uses are referred to as “session” cookies and “persistent” cookies. Session cookies are temporary and are automatically deleted once you close your internet browser. Persistent cookies remain on your computer hard drive or mobile device until you delete them or are otherwise removed upon expiration. Cookies are required for the online reservation process so that we can keep your information on multiple pages throughout the process. Additionally, Choice uses cookies to remind us of who you are, tailor our services to suit your personal interests, track your status in our promotions, contests and sweepstakes, and/or analyze your visiting patterns. Choice does not use cookies to ascertain any personally identifiable information about you apart from what you voluntarily provide Choice.

Choice may also use cookies to form an association between multiple devices such as your smartphone, desktop computer and tablet. This is often referred to as device fingerprinting. A unique identifier, or fingerprint, is created on your devices, which enables the association. Choice uses the device association to link your devices’ searches on our websites, which enables us to provide you with a more convenient and personal digital experience.

You can generally set your browser to not accept cookies or to notify you when you are sent a cookie, giving you the chance to decide whether or not to accept it. Not accepting cookies will adversely affect your ability to perform certain transactions and functions on Choice Websites.

Choice uses pixels or transparent GIF files to help manage its online advertising. These files enable Choice and its advertising partners to recognize unique codes on your web browser, which in turn, enable Choice to learn which advertisements bring users to its websites. The information that Choice collects and shares is anonymous and not personally identifiable. It does not contain your name, address, telephone number, or e-mail address.

Do Not Track Signals: Some web browsers offer a "Do Not Track" ("DNT") signal that is an HTTP header field indicating your preference regarding tracking or cross-site user tracking. We currently do not recognize DNT signals; however, we do allow you to exercise some choice in the information collected by adjusting your browser's cookie settings.

Google Analytics

This website uses Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to identify you as a unique user and help analyze how users use this site. The information generated by the cookie about your use of the website (including your IP address, but not your name of other identifying information) will be transmitted to and stored by Google on servers in the United States. This information is used for the purpose of evaluating your use of the website, compiling reports on website activity and providing other services relating to website activity and internet usage. The ad formats we utilize through Google include Audience Remarketing on Google's Display and Search Network.

You may refuse the use of cookies by selecting the appropriate settings on your browser. However, please note that if you do this, you may not be able to use the full functionality of this website. Furthermore, you can prevent Google's collection and use of data (cookies and IP address) by downloading and installing the browser plug-in available for various browsers located at https://tools.google.com/dlpage/gaoptout.

Additional information concerning Google's data privacy policy and other associated topics can be found at https://support.google.com/analytics/answer/6004245.

Do you use interest-based advertising?

Choice partners with third party ad networks to either display advertising on Choice websites or to manage its advertising on other sites. Choice's ad network partners use cookies and web beacons to collect non-personally identifiable information about your activities on Choice's websites and other sites to provide you targeted advertising based upon your interests. If you wish to not have this information used for the purpose of serving you targeted ads, you may opt-out by clicking here: http://preferences-mgr.truste.com. Please note this does not opt you out of being served advertising. You will still receive generic ads. Also, opting out of ad network cookies does not opt you out of cookies used for device association described in this privacy statement.

If you would like to know more about cookies, the website www.allaboutcookies.org provides useful information.

We also work with third parties that use tracking technologies on our Web sites in order to provide tailored advertisements on our behalf and on behalf of other advertisers across the Internet. These companies may collect information about your activity on our sites and your interaction with our advertising and other communications, and use this information to determine which ads you see on third party websites and applications. If you wish for more information about this practice and to understand your options, please visit www.aboutads.info.

Do you use my device's geo-location data?

Our mobile apps may use your device's Global Positioning System (GPS) or other technology to locate a hotel near you and/or to provide you with other relevant location-based information and/or services. Your location may be shared with Choice business partners to make services or products available to you, such as food delivery or local entertainment. While you have Choice's mobile app open, Choice and its business partners may track the device's precise location unless you have opted out of such sharing through your device's settings. When your device's location settings are turned off but the mobile app is open, Choice and its business partners may collect general location information (country, state, city) via IP address or other device information. The last location of your mobile device when the mobile app was open may be stored by Choice and/or its business partners for marketing purposes – for example, sending special offers to users whose last known location was in a particular city or region. Business partners who have access to your precise and/or general location information may use the information only in support of Choice's purposes described in this privacy policy.

To the extent any geo-location data is combined with personal information, that information will be treated as personal information in accordance with this policy.

What if I apply for a career at Choice Hotels on ChoiceHotels.com?

If you apply online for employment at Choice, you may be asked to provide us your name, address, e-mail and resume. Choice will use this information solely with respect to your job search and to determine your qualifications for a career with Choice.

Does this policy cover other sites linked from ChoiceHotels.com or Choice's Mobile Apps?

Choice is only responsible for the privacy and security policy and content on this website and Choice's mobile apps. ChoiceHotels.com and our mobile apps may redirect to other websites and mobile apps. Those websites and mobile apps are not covered by this privacy and security policy, and we are not responsible for the privacy practices or the content of those other websites and mobile apps.

What about changes to the Privacy and Security Policy?

By using our site you consent to our collection and use of your personal information as described in this policy. Choice reserves the right to modify this privacy and security policy and related business practices at any time by posting updated text on this site. Any changes to this policy

become effective upon posting of the revised policy to this site. Use of the site following such changes constitutes your acceptance of the revised policy then in effect.

What if I have questions or concerns?

Thank you for visiting our site and for taking the time to read this policy. If you have questions about this policy or complaints about how we collect, use, disclose, store or protect your personal information as directed by the laws and regulations applicable to your region, we can be reached by email at Privacy@ChoiceHotels.com or by writing to us at Choice Hotels International, Attention: Privacy Officer, 6811 E. Mayo Blvd., Suite 100, Phoenix, Arizona 85054.

How do you resolve complaints?

We will work with you to address complaints, which may include contacting applicable authorities as part of the resolution process.

What if there's a difference between versions of the Privacy and Security Policy?

As a service to our customers, we make this privacy and security policy available in several different languages. In the event of any discrepancies between the various translations of the policy, the English version of the policy is the authoritative one.