Entrepreneurs in Tech Breakfast Series:

CYBERSECURITY AND PRIVACY

09/27/2017

Michael Kasdan

WIGGIN AND DANA

Wiggin and Dana Entrepreneurs in Tech Breakfast Series

- **How To Protect Apps & Software with IP**
- **Start-up Primer on Corporate/IP Issues**
- **Cybersecurity and Privacy (Today!)**
- *Future Sessions in Our Series*:
  - **IP Issues for Start-ups**: How to both protect yourself and make money with your IP.
  - **How to Pitch Successfully**: what are investors looking for from early stage companies

WIGGIN AND DANA

- Mike Kasdan is a Partner in the IP Practice Group of Wiggin and Dana LLP and also a member of the firm's cyber-security and privacy practice group. He has a background in electrical engineering and technology consulting. He works with a broad range of technologies, including software, consumer electronics, wireless devices, computer architecture and networks, semiconductor chips, Internet and ecommerce platforms, and medical products and devices.
- He advises both mature and emerging companies. Since his time at NYU School of Law, Mr. Kasdan has been on the ground floor of efforts to turn New York City and State into a hub for innovation and entrepreneurship in technology, Internet, e-commerce and new media. He counsels new companies on legal, financing, business, and particularly intellectual property, contact-related issues, and privacy issues. He teaches as an Adjunct Professor at NYU Law School and speaks regularly at NYU Startup School.
- He previously served as Chairman of the Board of Directors of CityScience, a nonprofit organization promoting science, engineering, and math education in NYC schools, and writes and speakers on varied topics – including social justice, sports, politics, and mental health – for *The Good Men Project*.

WIGGIN AND DANA

Agenda/Discussion Roadmap

1. Privacy Policies and Terms of Use: Overview and Best Practices
2. Selected Recent Cases in Privacy and Takeaways
3. Location Tracking for Apps: Best Practices for Tech Companies
4. Data Collection in the Era of the IoT and Intelligent Products: Best Practices for Mitigating Privacy and Security Risk
5. Privacy and Security Risks in the Growing Use of Big Data Analytics: Emerging Best Practices

1. Privacy Policies and Terms of Service: Overview and Best Practices

- Basic Terms
  - Right to use posted or shared content
  - Content restrictions, prohibited uses, termination, removal
  - DMCA and notice and takedown compliance
  - Privacy and use of data

Tips and Best Practices

- Balance legal objectives with business objectives and user expectations
- Tailor terms to your business model
- Right to use licenses should obtain sufficient rights but not overreach
- Set up privacy and data-use policy that is both clear to users and tailored to business
- Clearly communicate key terms. Explain. In English.

2. Selected Recent Cases and Enforcement in Privacy: Takeaways

- Round-up of Recent Cases
  - *Standard Innovation* ('smart' vibrators) case on data collection
  - Facebook and Google cases on biometric privacy
  - Update on *FTC/Lab MD* case on data security
- FTC Privacy Enforcement Activity and Directions under the New Commission

Standard Innovation: Data Collection

- Standard Innovation, maker of 'smart' vibrators, settled a class action lawsuit earlier this year for $3.75M.
- Suit alleged "Standard Innovation collected individual-level usage information – often tied to users' personally identifiable addresses," they said, adding that the firm "breached its customers' trust, devalued their purchases" and "violated federal and state law in the process."
- **Takeaways**: Clear notice, security, disclosure/choice re: data shared by customers

We-Vibe: 'Smart' vibrator product allows users to remotely "turn on your lover" via Bluetooth connection using We-Connect mobile app.

Facebook and Google Cases: Biometric Data Collection

- *Licata et al. v. Facebook*
  - A number of Facebook users (now consolidated into a class) sued the social media giant in 2016 claiming it violated the Illinois Biometric Information Privacy Act of 2008 by collecting and retaining information about the geometry of users' faces from their uploaded photographs without written notice or informed consent.
  - The BIPA says no private entity can gather and keep an individual's "biometric identifiers" without prior notification and written permission from that person.

Facebook and Google Cases: Biometric Data Collection

- *Rivera et al. v. Google*
  - Similarly, a number of Google users in 2016 claiming it violated the Illinois Biometric Information Privacy Act of 2008 by automatically uploading plaintiffs' mobile photos and allegedly scanning them to create unique face templates (or "faceprints") for subsequent photo-tagging without consent.
- Takeaways
  - Both the *Facebook* and *Google* cases have survived motions to dismiss.
  - They are part of a recent wave of suits employing BIPA claims against social media and photo-sharing companies
  - Social media companies have sought to push back against the law, pushing an amendment that would specifically exempt physical and digital photographs and biometric information derived from them from BIPA.

Update on *FTC/Lab MD Litigation*: Limits on the FTC's Data Security Enforcement Authority?

- A grueling, epic litigation saga since 2013
  - The FTC's history of data security complaints under the "unfairness" prong of Section 5 of the FTC Act
  - Lab MD's basic challenge to enforcement authority
  - Where the case stands today
- Recent arguments before the 11th Circuit in June 2017
  - The court: FTC approach to Section 5 harms: "as nebulous as you can get"
- Implications of an FTC loss at the 11th Circuit

FTC Privacy Enforcement Activity and Directions under the New Commission

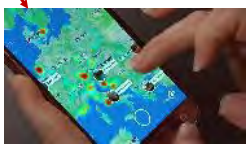
- **Commissioner Olhausen's Agenda for Privacy and Data Security Enforcement**
  - Section 5 unfairness focus on consumer harm and Commission "transparency"
- **Recent FTC Privacy and Security Actions and Takeaways**
  - *Uber* (data security/cloud/employee access)
  - *Lenovo* (OEM-installed adware compromising security)
  - *Taxslayer* (alleged Safeguards Rule violations in tax prep service)
  - *Blue Global* (failure to secure sensitive consumer information in deceptive loan application scheme)
  - *Credit Acceptance Corporation* (investigation re: use of GPS Data)

3. Location Tracking for Apps: Best Practices for Tech Companies

- What is the Issue?
- FTC and Industry Guidance
- Best Practices for Companies

What Is The Issue?

- Collecting and tracking geo-location data is increasingly a feature of mobiles devices and apps
  - Examples: Apple/Google, SnapChat Maps, Facebook, FourSquare



What Is The Issue?

- Tracking websites visited, consumer purchases, consumer attributes and behaviors enables access to very useful and private data
- Access to specific and continuous *geo-location* data enables tracking at an even deeper level
- Increase ability for advertisers/companies to target users based on their behaviors and locations in the world
- Increased “creepiness factor”?
- Safety issues re: presence in real world
- Concerns as to how companies and their partners use this very intimate data

FTC and Industry Guidance

- FTC Guidance
  - Basic Principles
    - Privacy by Design
    - Increased Transparency
    - Simplified Customer choice re data collected and shared
  - "Opt in" affirmative express consent (not opt out)
  - Clear just-in-time disclosures so customers understand what is collected/shared and with whom.
- Industry Self Regulation Guidelines
  - Digital Advertising Alliance (DAA): Transparency and Control
  - Network Advertising Initiative (NAI): Opt in consent and Reasonable Access to customer's own data

Best Practices for Companies

- Understand exactly how the tracking technology works, including what data it collects, where it sends data, and who can see the collected data. Establish robust privacy by design practices within the business.
- Conduct privacy impact reviews before using or deploying new tracking technologies.
- Privacy issues, like tracking consumers, are not just legal issues. They also impact customer relations.
  - When deploying tracking technologies, companies should consider industry best practices and customer expectations. Customer relations may require the company to go beyond what US law requires.
- Ensure all privacy notices or customer-facing statements accurately reflect the tracking technologies used.

Best Practices for Companies

- Before using tracking technologies to collect precise geolocations, biometric data or other highly sensitive personal information:
  - obtain the person's affirmative opt-in consent; and
  - establish data security measures appropriate to the data's sensitivity level.
- Companies using tracking technologies outside of the US must consider the impact of potentially stricter foreign data privacy laws.
  - The benefits of establishing uniform tracking technology and personal data use policies may lead a company to adopt a stricter procedure or policy approach than US laws require.
  - Foreign laws may also apply if companies transfer personal data across borders.

4. Data Collection in the Era of the IoT and Intelligent Products: Best Practices for Privacy and Security

- What is the Issue?
  - New class of devices collecting and using personal data in variety of ways
  - Billions of distributed, embedded, data-collecting, Internet-connected devices with little or no user interface for disclosing privacy practices

What is the Issue?

- Some Recent Examples
  - Roomba, IoT, automotive industry collection of data in cars, recent controversy of UnRoll.Me selling data, Google's recent decision to stop scanning email for ads
  - Cybersecurity botnet attacks such as Mirai attack, fall 2016

'Your Roomba May Be Mapping Your Home, Collecting Data That Could Be Shared' – NYT (July 25, 2017)

'Unroll.me Service Faces Backlash Over a Widespread Practice: Selling User Data' – NYT (April 24, 2017)

'Cars Suck Up Data About You. Where Does It All Go?' – NYT (July 27, 2017)

Recent Enforcement Activity/Legislation

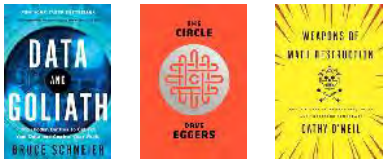
- Federal and state enforcement activity involving IoT
  - FTC cases: e.g., TrendNet, Asus, D-Link
  - New York AG: SafeTech Products settlement

- Proposed legislation
  - California's S.B. 37 ("Teddy Bear and Toaster Act")
  - U.S. Senate Bill, "Internet of Things (IoT) Cybersecurity Improvement Act of 2017"

Best Practices to Address Regulatory Scrutiny and Consumer Complaints

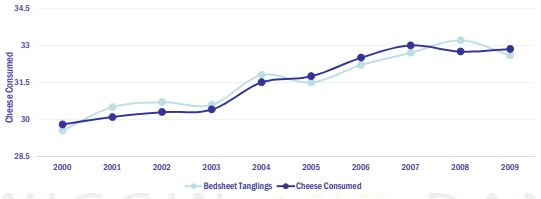
- Several U.S. federal agencies have offered compliance guidance for IoT market participants (e.g., NTIA, FTC, DHS, NIST)
- Guidance Highlights:
  - Follow "security by design" and "defense in depth" principles and build on recognized security practices
  - Stay on top of security patches and vulnerability management and communicate patch and update policies
  - Focus on secure authentication and secure interfaces with other devices and services
  - Default settings should favor consumer privacy and choice
  - Be transparent about data collection and use practices
  - Build communication channels with security researchers and users

5. Privacy and Security Risks in the Growing Use of Big Data Analytics: Emerging Best Practices



'Big Data' is Not Always 'Smart' Data

Per Capita Cheese Consumption
Correlates with
Number of people who died by becoming tangled in their bedsheets



Regulators are Paying Attention

NAIC
National Association of Insurance Commissioners

Black Letter Law

- What Laws Apply to Big Data Today?

Financial, healthcare, genetic and other data privacy and data security laws (state and federal)

State-regulations, such as insurance laws regulating underwriting, rating, claims handling

Anti-discrimination laws

Consumer protection laws

Gaps?

Basic Questions for Due Diligence and Risk Assessment in Data Analytics

What are the legal ground rules for using and sharing **internal customer data** in analytics projects?

What rules govern use of data sourced from **third-party sources** (e.g., data brokers, IoT devices, social platforms)?

How do we embed (i) **regulatory compliance** and (ii) **fidelity to our data policies** into algorithms and predictive models?

Who **owns** all of this data?

How do analytics projects affect our **cybersecurity risk**?

WIGGIN AND DANA

Best Practices: Ethics and Codes of Conduct

- Assure data quality and relevance
- Build in transparency, auditability of scoring models
- Prevent discriminatory impact and bias
- Demonstrate respect for consumer privacy
- Enforce accountability

WIGGIN AND DANA

Questions?

CYBERSECURITY AND PRIVACY

WIGGIN AND DANA

Contact Information:
Michael J. Kasdan
212.551.2843
mkasdan@wiggin.com

WIGGIN AND DANA

This presentation is a summary of legal principles.
Nothing in this presentation constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney.
The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

Michael J. Kasdan PARTNER

New York
212.551.2843
mkasdan@wiggin.com

EDUCATION

J.D., New York University School of Law
magna cum laude
Order of the Coif

B.S.E., University of Pennsylvania
magna cum laude

ADMISSIONS

New York

COURTS

US Court of Appeals for the Federal Circuit

US District Court (Eastern District of New York)

US District Court (Southern District of New York)

US Supreme Court

Michael is a partner in the firm's Intellectual Property Practice and is a member of the Diversity Committee. He has negotiated, defended and asserted IP rights in the numerous federal courts, the US Patent and Trademark Office, the International Trade Commission and in private arbitrations and mediations. As an advisor, he has worked with both established companies and start-ups to obtain, evaluate value, license and develop patent portfolios and trademarks.

Trained in electrical engineering and with a business background as a technology consultant, Michael works with a broad range of technologies, including consumer electronics, wireless devices, medical products and devices, computer architecture, software and networks, open source issues, semiconductor chips and Internet and e-commerce platforms.

His clients rely on him to resolve both large and small patent, trademark, and copyright cases efficiently and cost-effectively. For example:

- In a fast-moving ITC case, he spearheaded the two key claim construction issues for the joint defense group. The Administrative Law Judge took the unusual step of agreeing to stage the claim construction phase on potentially dispositive terms early in the case. The success in getting the Court to agree to an early claim construction phase drove favorable early settlements for numerous defendants.
- In a competitor semiconductor case brought as part of a global patent war involving the major electronics companies, he was instrumental in the defense of patent infringement claims and helped to obtain a jury verdict of non-infringement for his client.
- Michael was involved in the defense of a series of patent claims asserting infringement of mechanical processes, inspection processes and the materials structure of diaper and training pants products, among two competitors in the field.

Michael also counsels clients on strategic patent prosecution and portfolio development, and provides opinions and analyses on various patent issues, including patent infringement, validity and enforceability.

During 2008-2009, he was seconded to Panasonic Corporation in Japan. As in-house patent counsel in Panasonic's licensing center, he acted as lead counsel representing the company in numerous third-party patent assertions and license negotiations, where he was responsible for

Michael J. Kasdan **PARTNER**

developing substantive defensive positions. Michael also provided legal opinions across a broad set of technology areas and in many facets of patent law, and negotiated complex agreements, including portfolio cross-license agreements. In addition, he worked with the company's managers and engineers to identify high value patents and to strengthen their protection and mitigate exposure to infringement claims.

He frequently writes and speaks on a range of topics including IP litigation, standard essential patents, patent monetization, valuation and licensing practices, how to address IP issues for start-up and early stage companies, patent eligibility, patent exhaustion, willful infringement, patent misuse, patent valuation and inequitable conduct. Michael was interviewed on CNBC's public television *Nightly Business Report* regarding the Maps features of Snapchat and its privacy implications. His articles have been published in leading publications, including LEXIS, Practical Law Company, IP LAW 360, Bloomberg/BNA, and Managing IP Magazine. He is the sole author of Practical Law Company's *Practice Note on Patent Law* and the Lexis *Practice Advisor on Patent Licensing*. Michael was selected to author the chapter on Patent Licensing and Monetization of the *Oxford Handbook of Intellectual Property Law* (Oxford Press, 2017). Michael has also been the keynote speaker at conferences addressing topics such as diversity and mentorship.

Michael also teaches as an adjunct professor at his alma mater, NYU, as well as at New York Law School, addressing topics such as IP licensing, global patent litigation, patent exhaustion, and inequitable conduct. He has also guest lectured at the NYU Business and Law Clinic, the NYU School of Medicine, and at New York Law School and Seton Hall Law School. He clerked for the Honorable Judge Roderick R. McKelvie in the United States District Court for the District of Delaware.

Michael received his J.D. *magna cum laude*, from New York University School of Law. He was a member the NYU Law Review, the Order of The Coif, and was Fish & Neave Fellow for the Engelberg Center on Innovation Law and Policy, and served as President of the Intellectual Property and Entertainment Law Society. He is the Co-Chair of the Media Committee for the NYIPLA (NY IP Lawyers Bar Association) and also serves as a member of the Legislative Action Committee.

Michael also received a B.S.E. in Electrical Engineering, *magna cum laude,* from the University of Pennsylvania. He was a member of Eta Kappa Nu and Tau Beta Pi, Engineering Honor Societies, and a member of Penn Parliamentary Debate Team.

Outside of work, Michael serves as the Director of Communications and Development of the non-profit MyChild'sCancer. He also serves on the Board of the SouthNextFestival. He was formerly the Chairman of the Board of the non-profit CityScience, which focuses on improving STEM Education in our cities. He is also a contributor for *The Good Men* Project. He has spoken on a variety of issues on major media networks, including CNN Headline News, Al Jazeera America, NPR, and CBC Radio,

Michael J. Kasdan **PARTNER** and his writings have appeared in well-known publications such as *The Huffington Post*, *Salon, The BBC*, *The Daily Dot*, *Money* and *Redbook*.

How to draft terms of service online

What do Facebook, Microsoft and Pinterest get right, and wrong? **Michael Kasdan** and **Charles R Macedo** explain

For social media companies, internet companies, and others that have an interactive web presence, drafting effective terms of service is not a mere formality. Controversies with sites such as Pinterest, Dropbox and Facebook have illustrated the dangers of getting the terms, or the way they are communicated, wrong.

Crafting terms that are suited to a website's business requires the legal team to balance the necessary legal protections with both the businesses objectives and customer expectations. And while website providers are often tempted to look to existing agreements for boilerplate provisions, terms of service should not blindly pull provisions used by others. The terms that govern the relationship between a business and its users are necessarily fact-specific and depend on the relevant user base, how users are expected to interact with the website, and the relevant business model. One size cannot fit all.

One-minute read

The terms of service for social media companies, indeed any company with an interactive website, are increasingly important. They have to provide full legal protection for the company across a range of areas, including intellectual property, but also effectively and easily communicate those rights to users. As with any social media issues, a balance constantly has to be struck and several companies – such as Pinterest, Dropbox, No and Google Drive – have realised the business and PR costs of getting that balance wrong. Some have resorted to using plain language rather than legal terms. Others, such as Twitter, have taken a hybrid approach, which includes the full legal language but also prominently displays a plain English explanation.

Basic types of terms

Because every website should not necessarily have the same terms of service, it is useful to discuss the types of terms that should be considered rather than to suggest particular language. Accordingly, the following are some basic types of terms that should be considered:

Rights to use posted or shared content

Many websites allow users to post, upload or otherwise share content with other users. This could be pictures, videos, music presentations, commentary, lectures or virtually any kind of information. Without proper governance, the host website can open itself up to potential liability based on improper use of this content.

One issue that should be addressed is whether the terms of service ensure that the website obtains from the user appropriate rights for the intended (or perhaps even potentially unintended) uses of the content by the website.

Typically, terms of service will want to include some sort of limited licence to use that content in order to provide the service. The key issue here is the scope of that licence and how broad or limited it should be. Is the licence indeed limited to allow only that required to provide a service? Or is it necessary to obtain broader rights to use the data for other purposes? As this is dependent on the site's business model and what the company intends to do with the information, this should be given careful consideration. Furthermore, as discussed below, if the scope of a licence is perceived to be too broad, it can upset the user base.

One example of a limited licence is Microsoft's SkyDrive, which provides online or so-called cloud storage. Its terms of service plainly explain that:

> Except for material that we licence to you, we don't claim ownership of the content you provide on the service. Your content remains your content. We also don't control, verify, or endorse the content that you and others make available on the service.

It also very carefully limits the scope of Microsoft's content licence "solely to the extent necessary to provide the service":

> You understand that Microsoft may need, and you hereby grant Microsoft the right, to use, modify, adapt, reproduce, distribute, and display content posted on the service solely to the extent necessary to provide the service.

Seven tips on terms of service

1. Balance legal objectives with business objectives and user expectations
2. Tailor them to your business model; don't just use boilerplate terms
3. Right-to-use licenses for posted content should obtain sufficient rights for the business but not overreach
4. With provisions to address inappropriate content - including content that infringes third-party IP rights - always bear in mind what the user will tolerate
5. Minimise liability for third-party infringement by providing an appropriate notification procedure and internal response procedures in compliance with the DMCA
6. Set up a privacy and data-use policy that is both clear to users and tailored to your business
7. Clear communication of key terms to the user is paramount. Take the time to explain the meaning and rationale of terms

By way of comparison, Facebook's licence to user content in its 2009 terms of service raised controversy due to its breadth:

> You hereby grant Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide licence (with the right to sublicence) to (a) use, copy, publish, stream, store, retain, publicly perform or display, transmit, scan, reformat, modify, edit, frame, transmit, excerpt, adapt, create derivative works and distribute . . . any User Content you . . . Post . . . and (b) to use your name, likeness, and image for any purpose, including commercial or advertising, each or (a) or (b) on or in connection with the Facebook Service or the promotion thereof.

Clearly, while Facebook may have thought this was appropriate for its business model, this approach may not work for others. Indeed, Facebook itself no longer includes such a broad licence grant in its terms of service.

In drafting a content licence provision, it is important to understand what scope of rights is required, desired and acceptable for the business. If a limited licence is sufficient, it may be good not to overreach. On the other hand, if the business depends on the use of user-generated content or information, it is important to define the licence so that it is broad enough to provide the necessary rights. A site which generates revenue by republishing user content needs to obtain a broad enough license to cover such republication.

In addition to obtaining a licence from the user providing the content, the terms of service may also want the user to confirm that he or she has the right to grant a licence or obtained permission to share the content.

One way that terms of services may address this type of concern is by including representations and warranties by the user. For example, ScholarOne Manuscripts, a website used by publishers to obtain and process submissions by authors, includes in its terms of service the following representation and warranty:

> b. User owns, or has obtained all necessary right, licences and permission (i) to submit, upload, post, reproduce, distribute, and submit all User Submissions, including Manuscripts, via the Website utilizing the Software or the Services; and (ii) to grant ScholarOne, and Third-Party Users the licence and rights described below in this Section 6.

Content restrictions, prohibited uses, termination and removal

Another issue that platforms for user-generated content face is the posting of inappropriate content. For example, content may be disparaging, inflammatory, or perhaps infringe another's copyright, trade mark or other IP rights. This concern may be addressed in different ways.

First, as with the above example, the user can provide a representation and warranty that the content will not be inappropriate. ScholarOne includes a series of such representations and warranties:

> c. No User Submission, including any Manuscript, shall violate, misappropriate, or infringe the rights of any person or entity, including without limitation, any person or entity's trademark, patent, copyright, trade secret, intellectual property, statutory, proprietary, privacy, publicity, or contractual rights, or any other rights arising under the Laws of any applicable jurisdiction (collectively, "Third Party Rights").
>
> d. No User Submission, including any Manuscript, shall be unlawful, harmful, or threatening, or libelous or defamatory of any person or entity.
>
> e. All User Submissions, including any information concerning another person or entity, shall be true and accurate to the best of User's knowledge.

No doubt creative minds can come up with a laundry list of potential representations and warranties that could be included. Again, one should weigh this temptation against the business need for each term. Some users do not want to give up their first-born child just to submit a photo on a social network.

The site may also want to outline what content is inappropriate and expressly obtain the right to remove it. For this reason, terms of service often expressly set out content restrictions, prohibited uses, and provide rights for the site to remove

content or terminate use for violation. This may include, for example, a provision that prohibits the uploading or posting of content that is defamatory, obscene or otherwise unlawful.

Generally, this provision may also include a prohibition on posting anything that infringes IP rights. This may include copyrighted pictures, copyrighted text (such as news reports or blogs), trade mark infringement (including unauthorized fan pages) and postings of trade secrets.

In addition, terms of service may state that the user holds the site harmless and indemnifies it for any liability. Such provisions ensure that if content is suspected of being wrongfully provided it can be removed to limit exposure.

For example, the terms of service of Vimeo, a video sharing platform, provide:

> You may not upload, post, or transmit (collectively, "submit") any video, image, text, audio recording, or other work (collectively, "content") that: Infringes any third party's copyrights or other rights (e.g., trademark, privacy rights, etc.); Contains sexually explicit content or pornography (provided, however, that non-sexual nudity is permitted); Contains hateful, defamatory, or discriminatory content or incites hatred against any individual or group; Exploits minors; Depicts unlawful acts or extreme violence; Depicts animal cruelty or extreme violence towards animals; Promotes fraudulent schemes, multi level marketing (MLM) schemes, get rich quick schemes, online gaming and gambling, cash gifting, work from home businesses, or any other dubious money-making ventures; or Violates any law.

It also provides that "Vimeo may suspend, disable, or delete your account (or any part thereof) or block or remove any content you submitted if Vimeo determines that you have violated any provision of this Agreement or that your conduct or content would tend to damage Vimeo's reputation and goodwill". Again, it is important to consider not only what is needed and desirable from the website's perspective, but also what is acceptable for users.

DMCA and notice and takedown compliance

Another important consideration for websites that share content is minimising liability for infringement of third-party IP rights, defamation and harassment. For example, the Digital Millennium Copyright Act in the United States includes a safe harbour from copyright infringement claims for sites that host the content of others. To fall under the safe harbour, a service provider must implement notice and takedown procedures for infringing content.

In order to give rights holders an opportunity to address alleged copyright infringement, trade mark infringement and disparagement claims, the terms of service should provide a working notice system for third parties to contact the site to address concerns about specific posted content.

Many websites set up a mechanism to contact a dedicated resource that deals with claims of infringement. Depending on the site, this can range from a simple email notification to a designated department or agent, to a more streamlined set of online forms. In addition, the site should ensure it has an internal policy for promptly dealing with these complaints and removing offending content.

The bare minimum is to simply include a DMCA compliance notice that essentially states "we comply with the DMCA":

> It is the policy of [website] to promptly process and investigate notices of alleged copyright infringement, and take appropriate actions under the Digital Millennium Copyright Act, Title 17, United States Code, Section 512 ("DMCA").

Some users do not want to give up their first-born child just to submit a photo on a social network

The notice should also provide complainants with contact information and sets forth what information should be included in any complaint.

At the other end of the spectrum, Facebook's terms of service include a detailed page entitled How to Report Claims of Intellectual Property Infringement, with separate instructions and forms for copyright infringement and other claims. Using detailed forms can ensure the prompt and consistent collection of all necessary information. For example, the Facebook forms collect contact information, information on the infringement or objectionable content, an explanation of how it infringes, and a certification that the infringement claim is based on a good faith belief.

Privacy and use of data

Privacy and data security is another issue that is commonly addressed either in terms of service or a separate privacy policy that is referenced in the terms of service. There has been extensive litigation, threatened litigation and public criticism recently over how websites use, say they use, say they might use, or say they will not use data. This makes the issue not only a legal but a public relations issue as well.

The purpose of a privacy policy is to inform users how you collect and use their data. FTC guidelines require that websites that collect personal information have a "clear and concise" privacy policy that explains: what type of information the company or website collects, how the company or website uses that information, with whom the information is shared, and how the information is secured.

For example, the privacy policy of Wordpress.org, a popular blog, includes a section on the gathering of personally identifying information, which states that:

On managingip.com

- To tweet or not to tweet: advice on social media, May 2012
- Artists divided on Pinterest copyright threat, March 2012
- Social media: lessons from United Airlines and PwC, March 2012
- Tips on being social media counsel, January 2012

> Certain visitors to WordPress.org's websites choose to interact with WordPress.org in ways that require WordPress.org to gather personally-identifying information. The amount and type of information that WordPress.org gathers depends on the nature of the interaction. For example, we ask visitors who use our forums to provide a username and email address. In each case, WordPress.org collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor's interaction with WordPress.org. WordPress.org does not disclose personally-identifying information other than as described below. And visitors can always refuse to supply personally-identifying information, with the caveat that it may prevent them from engaging in certain website-related activities.

One avid Pinterest user who was a photographer and an attorney very publicly pressed the panic button

Other sections of the policy outline how this information is used, set forth the limitations on with whom this information may be shared, and address data security. As to data security, Wordpress's policy states that "WordPress takes all measures reasonably necessary to protect against the unauthorized access, use, alteration, or destruction of potentially personally-identifying and personally-identifying information".

Like the rest of the terms of service, it is important to specifically tailor your privacy policy to your business and business model. Be transparent, and draft a policy that the business is prepared to implement and abide by.

User controversies

Recent events have shown that once the terms of service have been drafted, it is also crucial to explain this set of rules to your users in an accessible way, whether in the terms themselves or elsewhere.

User controversy involving Pinterest and Google Drive illustrate this point. Both involved the inclusion of commonly used and important terms in their terms of service. Both highlight the importance of explaining these key terms to the user.

Pinterest.com is one of the fasting growing social media sites ever. Millions of users have joined its unique social media site, where users can share interests by virtually pinning images, videos, and other content to create online bulletin boards. If the pinned image or video originated on another website, that site may be accessed by clicking on the image or video.

Given that its business model relies on users posting content that often does not originate with them, minimising liability for potential copyright infringement claims is crucial.

Pinterest's terms of service stated that Pinterest's users are solely responsible for what they pin and that they must have express permission from the content owner to post any third-party content and included an indemnification and hold harmless clause. While these clauses are commonly found in the terms of service of most sites that allow users to post content (and for good reason), in the case of Pinterest it led to a blow-up. One avid Pinterest user who was a photographer and also an attorney very publicly pressed the panic button, concluding that the terms of service scared her so much that she shut down and deleted all of her Pinterest boards.

In the case of Google Drive, the user controversy involved the licence-grant provision in its terms of service that granted Google the rights to use and reproduce files stored by users in order to provide the service. The intent of the provision (also a common component of most terms of service) was to provide Google with only the rights necessary to provide its service. However, this provision was misunderstood by many users to mean that Google was obtaining unfettered rights in any and all of the content that is stored on Google Drive, which includes personal documents and photos, and that users no longer had ownership rights in that content.

The licence provision stated:

> When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide licence to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this licence are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones.

The terms of service also stated in another section that "Some of our Services allow you to submit content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours."

Taken together, these provisions provide a limited licence for the purpose of providing the service and make clear that the users retain ownership over content that is uploaded. Nonetheless, in looking at the licence provision or perhaps merely the first sentence of the licence provision in isolation, the user base was not so sure and feared that in uploading content, they were giving away their rights to Google.

Plain English or legalese?

A lesson here is that there is value in explaining the rationale behind and meaning of key terms and conditions – including the content licence and IP infringement prohibitions.

Indeed, spurred by such controversies, many companies have begun to supplement – or in some cases replace – their terms of service with plain English summaries. At the very least, the use of non-legalese, where possible and practical, is becoming recognised as a best practice. This is intended to demystify legal language and to explain in easy terminology exactly what the terms of service are.

Facebook moved to plain English terms of service in 2009, in response to user protests against its earlier terms, which users said were overreaching and difficult to understand.

Facebook's current terms of service include a section entitled "How we use the information we receive," which explains, in part, that "[g]ranting us this permission [to use user-generated content and data] not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways". This section also makes clear that "you always own all of your information."

In a more recent example, Dropbox, a competitor of Google Drive, had a similar controversy over its terms of service. Their users became upset over the licence language in the terms of service, which many feared provided Dropbox with IP rights in anything uploaded to the site. Dropbox's reaction was to explain, in plain English, that the licence was limited and that user's unquestionably "own their own stuff". They re-wrote the licence grant in plain English terms:

> By using our Services you provide us with information, files, and folders that you submit to Dropbox (together, "your stuff"). You retain full ownership to your stuff. We don't claim any ownership to any of it. These Terms do not grant us any rights to your stuff or intellectual property except for the limited rights that are needed to run the Services, as explained below . . . .

Dropbox's terms also plainly state that "we may need your permission to do things you ask us to do with your stuff, for example, hosting your files, or sharing them at your direction... You give us the permissions we need to do those things solely to provide the services."

Of course, in all cases, it is crucial to take care to ensure that the plain English is indeed readily understandable and, if used in the terms of service themselves (and not merely as a supplemental explanation) that it provides the intended rights and restrictions. If done properly, this practice can be useful in heading off controversy. Remember, however, that it is sometimes difficult to capture detailed legal concepts in plain English, and that if the dumbed-down version loses important concepts, this can result in liability, risk and exposure for the host.

Twitter's terms of service use a hybrid approach

Perhaps with such considerations in mind, Twitter's terms of service use a hybrid approach. They remain written in standard contractual language, but also include set-off boxes with explanatory plain English text. For example, the licence for Twitter to use user content states:

> You retain your rights to any Content you submit, post or display on or through the Services. By submitting, posting or displaying Content on or through the Services, you grant us a worldwide, non-exclusive, royalty-free licence (with the right to sublicence) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such Content in any and all media or distribution methods (now known or later developed).

However, this is followed by a set-off box that explains: "This licence is you authorizing us to make your Tweets available to the rest of the world and to let others do the same."

A corollary to providing plain English explanations and non-legalese is the placement and visibility of terms of service. Where transparency is important, consideration should be given to placing them in an accessible location. For example, Pinterest.com includes a link to Terms and Privacy and Copyright and Trademark in a large menu on the left of its About Pinterest page. These links bring the user to tabbed pages that include its Terms of Service, Privacy Policy, Acceptable User Policy, and Copyright and Trademark Infringement Complaint Forms.

Michael Kasdan

Charles R Macedo

© Michael Kasdan and Charles Macedo 2012. Both are partners at Amster, Rothstein & Ebenstein LLP in New York

Tracking Technologies: Privacy and Data Security Issues

MICHAEL KASDAN, WIGGIN & DANA LLP, AND MERAV SHOR, WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

Search the Resource ID numbers in blue on Practical Law for more.

A Practice Note providing an overview of the privacy issues surrounding common consumer tracking techniques, including online behavioral advertising, mobile device and precise geo-location tracking, geofencing, and facial recognition.

With the advent and widespread adoption of tracking technologies, consumers encounter privacy issues every time they go online, use their cell phone, or wear a connected device. Many companies track consumers' online behavior or allow others to do so, mainly for the purpose of behavioral advertising or providing user-targeted services. Companies may collect information on:

- What websites consumers visit.
- What consumers search for online.
- What consumers shop for, both online and in stores.
- Their consumers' exact current and past locations.
- Their consumers' physical activities or attributes, such as the number of steps walked or a resting heartrate.

In the past, most consumer tracking occurred on a stationary computer or personal laptop with limited mobility. Today, technology advancements leading to smaller but more powerful computing devices, improvements in sensor devices, and the pervasiveness of mobile computing, generate the potential for constant tracking, both on and across a wide range of devices including consumers' mobile phones, tablets, smart phones, smart watches, and other wearable devices.

Many companies have the technical capability to collect personal information (also known as personally identifiable information or PII) on an individual basis. Companies may also supplement this information with data collected from other sources, including public records and social media accounts, like Facebook, LinkedIn, or OK Cupid, where consumers often openly post their names, pictures, hometown, lists of friends and relatives, age, religious beliefs and political views.

Rapid technology changes often also raise potential privacy concerns, as the technical ability to act outstrips the law's ability to adapt or provide guidance. Consumer attitudes and concerns are also hard to measure with the fast pace of innovation and the number of market actors. Spotting violations, enforcing existing rules, and simultaneously developing new counter-tools to address emerging practices that may harm consumers is extremely challenging.

Companies leveraging new tracking technologies must find ways to both accomplish their business goals and comply with evolving privacy laws and regulations. However, companies can mitigate these challenges by providing consumers with transparency, disclosure, and choice to control how their data is used.

This Note discusses:

- The general legal framework governing privacy in the US.
- Common consumer tracking mechanisms.
- The legal and industry self-regulation frameworks applicable to each common consumer tracking mechanism.
- Best practices when companies deploy consumer tracking mechanisms.

THE US PRIVACY REGULATORY FRAMEWORK

Unlike many other countries, the US does not have a comprehensive data protection law or framework that regulates consumer data privacy protection. The US instead follows a sectoral approach to privacy. This approach provides more context-specific legislation and regulation, but leaves gaps and creates a patchwork regulatory regime that is complicated to understand, comply with, and enforce. Companies using tracking technologies in the US must consider:

- General consumer privacy laws and regulations (see The Federal Trade Commission).
- Sector specific privacy laws (see Sector Specific Legislation and Regulatory Provisions).
- State privacy laws (see State Legislation).
- Self-regulatory frameworks (see Industry Self-Regulation).

THE FEDERAL TRADE COMMISSION

In the US, the Federal Trade Commission (FTC) serves as the primary regulator for consumer privacy. The Federal Trade Commission Act grants the FTC the authority to regulate "unfair or deceptive" practices. These practices may arise, for instance, where companies make false or misleading claims about privacy or data security practices or fail to apply reasonable security measures that cause or are likely to cause significant consumer harm. The FTC can take action against companies that mislead consumers about their compliance with a self-regulatory scheme by asserting a deceptive practice under the FTC Act. State attorneys general hold similar powers and collaborate with the FTC in these enforcement endeavors (see State Legislation and Box, Tracking-Related Federal and State Enforcement Actions).

The FTC's General Privacy Guidance and Recommended Best Practices

The FTC also issues privacy and data security guidance that, while not legally binding, provides businesses with best practices and insight into the FTC's enforcement priorities. For example, in its 2012 report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (FTC Protecting Consumer Privacy Report), the FTC laid out a set of general privacy framework best practices, encouraging businesses that collect and use consumer personal information to follow these three baseline principles:

- **Privacy by design**. The FTC encouraged companies to incorporate and consider consumer privacy and data security protections at every stage of the product, process, and policy development cycle (see Practice Note, Developing a Privacy Compliance Program: Box, Privacy by Design (5-617-5067)).
- **Simplified consumer choice.** The FTC advocates for providing consumers with clear and simple choices about how the company intends to use their personal information when the company collects it. While all consumer data collections and uses may not require consumer choice, companies should provide choices for practices that may surprise consumers or are inconsistent with the context of the customer relationship, including:
  - tracking consumer behavior across other parties' websites;
  - sharing information with third parties, including affiliate relationships not clearly recognized by consumers;
  - collecting or using sensitive personal information, like health data or other information that may lead to embarrassment, discrimination, or consumer harm; and
  - making material retroactive changes to privacy representations.
- **Greater transparency.** The FTC encouraged increased transparency of personal information privacy practices including:
  - using clear, short, and standardized notices that effectively allow consumers to understand and compare privacy practices;
  - providing consumers with reasonable access to the information held about them that is proportional to the data's sensitivity and intended use; and
  - providing better consumer education about commercial data privacy practices.

Particularly relevant for most tracking programs, the FTC has cautioned that businesses must adequately notify individuals of any personal information collection and sharing practices:

- That may not be obvious to the consumer, for example, automatic data collection methods, cross-device tracking, or sharing data with a third party unrelated or unnecessary to the consumer's business relationship.
- That are materially different from those disclosed in the privacy notice.
- Before materially changing the privacy notice.

Tracking-Specific FTC Reports

The FTC has also issued several reports addressing the unique aspects of specific consumer tracking techniques, including:

- Cross-Device Tracking, FTC Staff Report, January 2017 (FTC Cross-Device Tracking Report) (see Device Fingerprinting and Cross-Device Tracking).
- Self-Regulatory Principles for Online Behavioral Advertising, FTC Staff Report, February 2009 (FTC OBA Report) (see Online Behavioral Advertising).
- Mobile Privacy Disclosures: Building Trust Through Transparency, FTC Staff Report, February 2013 (FTC Mobile Privacy Report) (see Mobile Device Tracking).
- Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies, FTC Staff Report, October 2012 (see Facial Recognition and Biomarkers).
- Data Brokers: A Call for Transparency and Accountability, FTC Staff Report, May 2014 (FTC Data Broker Report) (see Data Brokers and Combining Data from Multiple Sources).
- Internet of Things: Privacy & Security in a Connected World, FTC Staff Report, January 2015.

FTC Enforcement Powers

Section 5 of the FTC Act also grants the FTC powers to issue administrative complaints. The FTC claims this authority extends to privacy and cybersecurity violations, when companies fail to protect consumers' personal information adequately, because they result in unfair business practices that trigger its Section 5 regulatory authority. However, some legal experts consider the FTC's position controversial as it stretches the typical antitrust definition of unfair or deceptive business practices. Currently, the FTC asserts its Section 5 authority to pursue companies that:

- Fail to implement a data security program.
- Violate the terms of their data privacy policies.
- Expose personal information in a data breach.
- Misrepresent information or practices in their privacy policies.
- Experience security lapses that lead to privacy policy misrepresentations.

Due to high litigation costs and reputational harm, most companies settle privacy or data security related charges with the FTC by using consent decrees. For more on the FTC's data security standards and enforcement actions generally, see Practice Note, FTC Data Security Standards and Enforcement (8-617-7036).

The FTC has taken an active role in investigating and exposing privacy violations related to consumer tracking mechanisms, particularly when the tracking activities are hidden or undisclosed. For more on tracking-specific enforcement actions, see Box: Tracking-Related Federal and State Enforcement Actions.

SECTOR SPECIFIC FEDERAL LEGISLATION AND REGULATORY PROVISIONS

While the FTC provides general consumer privacy guidance, other federal statutes establish specific privacy practices and requirements for different industry sectors or activities. Companies conducting tracking operations in these sectors must consider the impact of sector-specific statutes when developing their programs. Relevant sectors include:

- **Healthcare.** The Health Insurance Portability and Accountability Act (HIPAA) and related amendments in the Health Information Technology for Economic and Clinical Health Act (HITECH) address the use and disclosure of an individual's protected health information by specified "covered entities," and includes standards designed to help individuals understand and control how their health information is used. Only using or disclosing the "minimum necessary" protected health information represents one of HIPAA's key principles (see Practice Note, HIPAA Privacy Rule (4-501-7220)). HIPAA and HITECH's implementing regulations also extend to a covered entity's "business associates," which include third-party service providers performing functions or services for a covered entity that involves protected health information. HIPAA's requirements extend to all similarly situated downstream contractors.
- **Financial services.** The Gramm-Leach-Bliley Act (GLBA) mandates that financial institutions respect their customer's privacy and protect the security and confidentiality of those customers' nonpublic personal information. It requires financial institutions to issue privacy notices to their customers that explain their information sharing practices and give customers the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules (4-578-2212)).
- **Consumer credit and background checks.** The Fair Credit Reporting Act governs the conduct of consumer reporting agencies that provide consumer data for purposes of making decisions on credit, employment, insurance, housing, and similar eligibility determinations. It generally does not cover the sale of consumer data for marketing and other purposes (see Practice Note, Understanding the Fair Credit Reporting Act (FCRA) (w-001-8260)).
- **Children's privacy.** The Children's Online Privacy Protection Act (COPPA) prevents the online collection of personal information about children younger than 13 without a parent's consent. The FTC's regulation implementing COPPA established additional requirements directed at internet operators, including the obligations to:
  - post a clear online privacy policy detailing information practices for personal information collected from or about children under 13 years old;
  - reasonably provide direct notice to parents of those practices;
  - obtain verifiable parental consent before personal information collection;
  - provide reasonable means for parents to review the personal information collected and to refuse to permit its further use/maintenance; and
  - only retain a child's personal information for the time necessary to fulfill its original collection purpose.
- For more on COPPA's requirements, see Practice Note, Children's Online Privacy: COPPA Compliance ((1-555-6526)).
- **Education.** Two federal statutes provide the primary federal protections for a student's personal information held by educational agencies and institutions that receive federal funding:
  - the Family Educational Rights and Privacy Act (FERPA) restricts the disclosure of education records; and
  - the Protection of Pupil Rights Amendment (PPRA) restricts the use of surveys, evaluations and similar exams. It also restricts the collection and use of student personal information for marketing purposes.
- Many state laws also restrict the use of student personal information collected using online tracking mechanisms (see State Legislation). For more on federal and state student privacy protections, see Practice Note, Student Privacy: Education Service Provider Requirements (w-001-1128).
- **Telecommunications carriers.** The Federal Communications Commission (FCC) regulates telecommunication carriers and services to protect the privacy of customer proprietary network information (CPNI) under the Communications Act (47 U.S.C. § 222; 47 C.F.R. § 64.2001 to 64.2011). CPNI may include personally identifying information that can track a customer's behavior (see Verizon Wireless FCC Supercookie Settlement).
- **The Video Privacy Protection Act (VPPA).** This statute originally intended to limit the conditions under which a video rental or sales outlet may disclose personally identifiable information about consumers, including their viewing history. While newer technologies like DVDs and streaming video have practically replaced video tapes, the law's broad language extends its application to similar audio-visual materials. Consumers have the right to opt-out from disclosure of their name and address, for example, as part of a mailing list. Consumers harmed by a VPPA violation can also sue for actual damages, punitive damages, and attorneys' fees and costs. Congress amended the law to enable internet sites like Facebook and Netflix to share the consumer's viewing history with their written consent.
- **The Genetic Information Nondiscrimination Act (GINA).** This statute protects individuals from genetic discrimination in health insurance and employment. It defines genetic discrimination as the misuse of genetic information, which includes:
  - family health history;
  - genetic test results;
  - the use of genetic counseling and other genetic service; and
  - participation in genetic research.
- For more on GINA's requirements, see Practice Notes, Discrimination Under GINA: Basics (4-615-0265) and GINA Compliance for Health and Welfare Plans (5-521-7266).

- **Workplace monitoring**. Employers increasingly rely on emerging technologies to help monitor employee behavior for a variety of reasons, including the potential to minimize legal risks from employee behavior, such as inappropriate internet activity or unauthorized disclosure of a customer's personal information. For more on workplace monitoring, see Practice Note, Electronic Workplace Monitoring and Surveillance (1-506-8862).

STATE LEGISLATION

At the state level, privacy legislation takes several forms, including state "mini-FTC Acts" that prohibit companies from committing a deceptive business practice. Similar to the FTC Act, these statutes provide a legal basis for states to protect their consumers' privacy, including from inappropriate or undisclosed consumer tracking (see Box: Tracking-Related Federal and State Enforcement Actions).

Other common state privacy legislation includes:

- Security standards or safeguard requirements that govern the personal information retained when companies conduct consumer-tracking activities (see Practice Note, State Data Security Laws: Overview (w-002-2498)). These safeguards often include requirements for data destruction, retention, and classification.
- State data breach notification statutes that require notification when an unauthorized disclosure occurs involving the personal information of a state resident (see Data Breach Notification Laws: State Q&A Tool).

For more on California's privacy and data security laws, which are among the most protective in the US, see Practice Note, California Privacy and Data Security Law: Overview (6-597-4106).

Student Privacy

States have also taken a leading role in protecting student privacy, passing comprehensive statutes, such as California's Student Online Personal Information Protection Act (SOPIPA) (see Practice Note, Student Privacy: Education Service Provider Requirements: California Student Privacy Laws (w-001-1128). Among other items, California's SOPIPA restricts what companies can do with student personal information collected using online tracking mechanisms, prohibiting services covered by the statute from:

- Engaging in targeted advertising on the service.
- Using covered information for targeted advertising on other locations.
- Developing student profiles using covered information for a non-K-12 school purpose.
- Selling covered information to third parties (except as part of a merger or business sale).

(Cal. Bus. & Prof. Code 22584(b), (e).)

Companies operating in the educational technology industry should carefully review the relevant state student privacy restrictions before implementing programs that track student activity or behavior. For more on state student privacy legislation and requirements, see Student Privacy: Education Service Provider Requirements: State Student Privacy Laws (w-001-1128).

INDUSTRY SELF-REGULATION

Self-regulatory industry bodies have also played a significant role in regulating US internet and mobile ecosystems. When done well, self-regulation can be good for both consumers and industry because it often adapts to changing technologies more quickly than government statutes or regulation. It also enables industry experts that may better understand the industry and changing technologies to account for market needs when tailoring the rules for specific applications. Industry groups providing self-regulatory guidance on a variety of online tracking issues include:

- The Digital Advertising Alliance (DAA) self-regulatory framework consisting of:
  - the Self-Regulatory Program for Online Behavioral Advertising (see Online Behavioral Advertising);
  - the Application of Self-Regulatory Principles to the Mobile Environment;
  - the Self-Regulatory Principles for Multi-Site Data; and
  - the Application of the DAA Principles of Transparency and Control to Data Used Across Devices (see Device Fingerprinting and Cross-Device Tracking).
- The Network Advertising Initiative (NAI) self-regulatory framework consisting of:
  - the NAI Code of Conduct (2015 Update) (see Online Behavioral Advertising);
  - the NAI Mobile Application Code of Conduct (2015 Update) (see Mobile Device Tracking);
  - the Use of Non-Cookie Technologies for Internet-Based Advertising guidance; and
  - the Cross-Device Linking guidance (see Device Fingerprinting and Cross-Device Tracking).
- The Groupe Spéciale Mobile Association's (GSMA):
  - Mobile Privacy Principles; and
  - Privacy Design Guidelines for Mobile Application Development.
- The Future of Privacy Forum (FPF) guidance for:
  - Mobile Location Analytics Code of Conduct (see Geofencing); and
  - Best Practices for Consumer Wearables and Wellness Apps and Devices.
- National Telecommunications and Information Administration (NTIA) guidelines for:
  - Code of Conduct for Mobile App Transparency; and
  - Privacy Best Practice Recommendations For Commercial Facial Recognition Use (see Facial Recognition and Biomarkers).

INTERNATIONAL CONSIDERATIONS

Compliance with foreign privacy and data protection requirements is outside the scope of this Note. However, US-based businesses collecting personal information from residents of non-US jurisdictions or operating in foreign jurisdictions by, for example, serving online behavioral advertising to residents located in non-US jurisdictions, may be subject to privacy and data protection laws in those jurisdictions.

The privacy and data security laws of certain jurisdictions, including those adopted by the European Union (EU) member states under the EU Data Protection Directive (Directive) and the recently approved General Data Protection Regulation (GDPR) (effective May 25, 2018), are more stringent than US laws. They also may require user consent for certain data collection techniques, such as the use of cookies (see Internet Cookies), or restrict transfers of personal information outside that jurisdiction (see Practice Note, Drafting Privacy Notices: Box: Transferring Personal Information from the EU to the US (w-000-9621)). For additional information on privacy and data protection laws in selected non-US jurisdictions, see the Data Protection Global Guide. For more on the EU's data protection laws, see Practice Notes, Overview of EU Data Protection Regime (8-505-1453) and Overview of the EU General Data Protection Regulation (w-007-9580).

TRACKING METHODS AND COMMON USES

INTERNET COOKIES

Traditionally, websites tracked a visitor's website interactions by placing data files on the computer, called "cookies." Cookies allow websites to remember information about a visitor and enable a wide variety of website functions, including:

- Keeping the user securely logged into their account.
- Tracking shopping cart items.
- Remembering preferences or settings.
- Customizing browsing activity or targeting that user with advertisements (see Online Behavioral Advertising).
- Creating visitor profiles based on past activities.

Websites can place cookies on a users' computer from the actual website the person visits or from third parties, such as an advertiser, content recommender, or social media plug-in. These third-party companies can then track sites that the user normally visits to target that user with ads or analyze preferences to learn more about the site's use (see Online Behavioral Advertising).

Adobe's Flash player uses a similar technology to store user information known as Flash cookies. Unlike internet cookies, Flash cookies are stored outside of the browser, which allows multiple browsers on the same computer to access them. Flash cookies can also store more data than internet cookies.

Websites written using the most recent version of the hypertext markup language, HTML5, can also leverage local storage options that provide similar cookie functionality, but with improved speed and security, known as HTML5 cookies.

Unlike other jurisdictions, such as the EU, US privacy laws do not set blanket notice and consent requirements for all cookie uses. Rather, the US privacy requirements depend on what type of information the cookie collects and how the website operator permits companies to use or share that information (see FTC Protecting Consumer Privacy Report).

For example, websites using cookies for internal website functions and other purposes consistent with the context of the website visitor's relationship, such as secure logins, authentication, or ecommerce features, typically do not require more than a general privacy notice disclosure about their use. However, websites employing cookies to track users in unclear or non-obvious ways, particularly for uses that track browsing activity over time or across websites, or that share browsing activity with third parties, should, at minimum:

- Disclose the cookie's use and tracking activity, including any third-party data sharing or uses.
- Provide instruction on how to opt-out of or block the tracking activity.
- For sensitive personal information collections or use, obtain the person's affirmative express consent.

Cookies used for OBA related purposes should also follow the relevant self-regulation guidelines (see Online Behavioral Advertising). A company using cookies or other tracking software should also disclose those practices in its privacy policy. Otherwise, the FTC or a state regulator may consider the company's data privacy program inadequate.

Users can limit a cookie's effect using their web browser settings. Depending on the specific browser's settings, consumers can choose to delete certain cookies or limit the types of cookies permitted, such as by blocking third-party cookie use. However, simply instructing website visitors to delete or block cookies does not provide a true opt-out solution that satisfies legal or self-regulatory guidelines, as:

- Deleting individual cookies does not stop all tracking activities. Unless the consumer completely blocks all cookie use, the website can simply set a new tracking cookie during the next visit.
- Entirely blocking all cookies often negatively affects a consumer's overall browsing experience by preventing useful and important website functions. For example, blocking all cookies may:
  - prevent a website from recognizing a frequent visitor;
  - require the reentry of data or creation of new accounts;
  - prevent websites with more complex programming, such as online stores, from processing an order; or
  - lose the option of receiving meaningful personally tailored content.
- Directing a person to delete cookies from their browser does not necessarily delete Flash cookies. Companies using Flash cookies to track user behavior should provide specific instructions on how to delete them or opt-out of their continued use.

For a model website privacy notice containing cookie disclosures, see Standard Document, Website Privacy Policy (2-501-2704).

DEVICE FINGERPRINTING AND CROSS-DEVICE TRACKING

Technology advances have led to new digital tracking methods that do not employ traditional website cookies, including device fingerprinting and cross-device tracking. Companies can configure these improved technologies to track consumers across the various devices they use simultaneously, a feature not available with traditional cookies that only operate within individual bowsers.

Device fingerprinting works by collecting and analyzing the configuration settings, metadata, and other information a device sends out when connecting to the internet, like the IP address, browser versions, or the available font sets. These data elements individually do not provide unique identifications. However when combined, they generate statistically relevant device "fingerprints" capable of uniquely

identifying individual device interactions across time and over different websites. Companies can then create profiles designed to recognize returning devices and track their activity over time.

Consumers often use more than one internet-connected device, moving between their mobile phone, tablet, smart watch, laptop, and home computer. Cross-device tracking enables companies to associate these different devices with a single individual, either conclusively or with a high degree of probability. Cross-device tracking typically uses one of two techniques:

- **Deterministic identification**, which relies on login or other information the user enters on multiple devices to link them. For example, when a consumer logs into their email account on different devices, such as a laptop and mobile phone, the email service provider can link those devices to their identified consumer.
- **Probabilistic identification**, which analyzes data collected from different devices to look for common patterns, such as a common IP address and location, to conclude that the same person or household uses those devices.

In the age of the Internet of Things, many home appliances and smart devices can also connect to the internet, often times using the same IP address (see Practice Note, The Internet of Things: Key Legal Issues (w-002-6962)). For example, smart entertainment systems may track the TV shows watched on them. Cross-device tracking allows companies to connect that TV viewing data with internet searches or data collected from the TV viewer's other devices.

However, companies must take care when tracking a consumer's media consumption habits. In early 2017, Vizio, an internet-connected TV manufacturer, installed software on its TVs that automatically tracked a customer's viewing habits. Vizio then used the viewing habit information to engage in targeted advertising until the FTC and certain state attorneys general brought suit claiming the tech company violated privacy laws because it did not adequately disclose the practice or obtain consent (see Box: Tracking-Related Federal and State Enforcement Actions).

In January 2017, the FTC issued a Cross-Device Tracking report discussing the application of its general privacy principles to cross-device tracking activities (FTC Cross-Device Tracking Report). It recommends that companies engaging in cross-device tracking:

- Transparently disclose their cross-tracking activities and tracking practices including actions that enable third-party cross-device tracking.
- Provide clear, comprehensive, and meaningful disclosures about probabilistic tracking methods used by companies without a direct consumer relationship.
- Make truthful claims about the categories of data collected, including not characterizing or referring to raw or hashed email addresses or user names as anonymous or aggregate data. For more on the pitfalls of hashing as an encryption technique, see FTC: Does Hashing Make Data "Anonymous"?.
- Not make blanket statements claiming the company does not share personal information with third parties if it provides raw or hashed email address or user names to cross-device tracking companies or otherwise shares data reasonably linked to a consumer or a consumer's device.
- Provide consumers with control over data tracking by using choice mechanisms that:
  - clearly and conspicuously disclose any material limitations on how the provided opt-out tools apply or work;
  - simplify consumer opt-out methods and choices when technically possible; and
  - honor a consumer's behavioral advertising opt-out choice on one device by preventing that device from both receiving behavioral ads based on information from other devices or informing behavioral ads on other devices.
- Establish heightened protections for sensitive information, such as health, financial, precise geolocation, and children's information, including collecting or using that data only with the consumer's express opt-in consent.
- Establish reasonable security for collected data, including keeping only data that is necessary for the company's business purposes.

The FTC's report warns that a cross-device tracking company's failure to truthfully and fully disclose information about its tracking practices to both consumers and other companies using or enabling the cross-device tracking technology may violate the FTC Act.

Industry Self-Regulation

The DAA also released a cross-device tracking report in November 2015 entitled, Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices. The DAA's report identified two norm-based principles to help guide a company's use of data across devices or apps:

- **Transparency.** A company must ensure consumers are aware of its cross-device practices by providing a clear, meaningful, and prominent link to a disclosure in the privacy policy or on the website that describes control mechanisms.
- **Control.** This principle emphasizes that consumers must have the option to limit the collection and usage of cross-device or app tracking.

Together, the DAA expects these principles to frame a company's approach to data security practices when dealing with cross-device tracking.

ONLINE BEHAVIORAL ADVERTISING

Online behavioral advertising (OBA), sometimes referred to as interest-based advertising (IBA), represents one of the most common uses for online tracking data. Companies use data collected using different tracking technologies to generate profiles for different internet users that attempt to predict the person's interest from their past activity. Targeted ads based on a consumer's browsing history may appear in completely unrelated sites that the person visits for the first time. For example, OBA technologies may cause a website visitor frequently reading food recipes to receive ads about kitchen appliances while visiting a car website for the first time.

The FTC issued a report in 2009 concerning self-regulatory recommendations for OBA, which it defined as the tracking of a consumer's online activities over time or across different websites to deliver advertising tailored to the individual consumer's interests, including:

- The searches conducted by the consumer.
- The web pages visited.
- The content viewed.

(FTC OBA Report, February 2009.)

The FTC OBA Report laid out the following four self-regulatory principles companies should follow when tracking user activity for OBA related activities:

- **Transparency and consumer control**, which requires websites collecting OBA-related information to provide consumers with:
  - information about their collection practices in a clear, concise, consumer-friendly, and prominent statement; and
  - choice about the collection and use of their information in a clear, easy to use, and accessible way, such as the advertising icon adopted by the DAA.
- **Data security and retention**, which requires that companies provide reasonable security measures for any OBA related data collected that prevents it from falling into the wrong hands and to keep this data only as long as necessary for legitimate business or law enforcement needs. Companies should customize the security measures based on:
  - the collected data's sensitivity;
  - the nature of the company's business;
  - the types of risks that the company faces; and
  - the reasonable protections available.
- **Opt-in consent for retroactive changes**, which requires obtaining a consumer's affirmative express consent before using OBA related data in a manner that is materially different from the company's privacy policy statement in effect when it collected the data. Express affirmative consent requires the consumer's affirmative action, such as clicking an "I Agree" button or checkbox.
- **Opt-in consent for the use of sensitive data,** which requires obtaining a consumer's affirmative express consent before using sensitive data for OBA purposes. Sensitive data generally includes:
  - financial and health data;
  - Social Security numbers;
  - information concerning children; and
  - precise geographic location.

However, the report's recommendations did not cover consumer tracking conducted directly by the website owner about activity on that site, known as first-party tracking, when the first party:

- Does not share the collected information with third parties or participate in an OBA network.
- Only used the collected data for:
  - improving that website; or
  - contextual advertising, that selects the displayed ad based on the web page's or specific search query's content, instead of a user profile.

Several advertising industry groups also have developed self-regulatory frameworks addressing OBA that most online advertisers, ad tech, and ad network companies follow (see Practice Note, Online Advertising and Marketing: Voluntary Regulations and Codes of Practice (4-500-4232)).

The NAI and DAA operate the two primary OBA self-regulatory frameworks in the US. For more on these voluntary codes, see Practice Note, Online Advertising and Marketing (4-500-4232).

Program participants must also agree to industry-backed enforcement processes. For example, the Advertising Self-Regulatory Council (ASRC) took enforcement actions against three mobile app providers that were not complying with the DAA's OBA self-regulatory principles in May 2016 (Legal Update, Mobile App Publishers Agree to Comply with Digital Advertising Alliance Self-Regulatory Principles (w-002-2338)). The NAI also operates a similar code enforcement program (see NAI: Enforcement).

To provide transparency to consumers around OBA, the DAA, and the NAI have also developed the AdChoices program that offers consumers an opt-out tool and information on how the advertiser uses their data. Participating advertisements display the ubiquitous Ad Choices little blue triangle icon. Clicking the icon brings consumers to the advertiser's information and opt-out page.

For more on digital advertising best practices, including OBA, see Practice Note, Online Advertising and Marketing (4-500-4232).

MOBILE DEVICE TRACKING

Mobile devices offer a wealth of individual tracking opportunities due to their wide range of sensors and constant presence near their owners. Cookies have limited usefulness in a mobile driven world. Instead, mobile devices often track user behavior with more sophisticated technologies, such as device fingerprinting and cross-device tracking (see Device Fingerprinting and Cross-Device Tracking). Device identifiers, such as Apple iOS's Identifiers for Advertisers ("IDFA") and Google Android's Advertising ID, are another kind of technology that allows device tracking enabled through a consumer's use of apps. Marketers often use device identifiers to monitor the various apps used on a certain device.

The FTC issued its Mobile Privacy Report in February 2013. The report discussed the unique privacy challenges generated by mobile devices and built on the FTC's general privacy framework discussed in its prior Protecting Consumer Privacy Report. It also presented a set of suggested best practices for applying the privacy framework to the mobile world.

While the FTC Mobile Privacy Report directed many of its recommendations to the large mobile platform providers, such as Apple, Google, Amazon, Microsoft, and Blackberry, because of their power as "gatekeepers" to the data their devices generate, it also contained specific privacy recommendations for companies leveraging the device's tracking capabilities.

Companies developing mobile apps that track the device owner's actions or activities should:

- Provide privacy notices disclosing the tracking activity and data uses in plain and clear language that avoids technical jargon.
- Make those notices available before the device owner downloads the app.
- Obtain the device owner's affirmative express consent using just-in-time disclosures before collecting, accessing, or sharing sensitive information, including the device's:

  - geo-location information (see Tracking Precise Geolocations and Geofencing);
  - photos;
  - audio or video recordings;
  - contact lists and calendar entries; and
  - data outside of the platform's application programing interface (API) that reveals sensitive information, such as queries about health conditions, financial data, or biometric information from the device's sensors.
- Understand exactly what the app does with the device's data, including where the app sends the data, particularly when incorporating code or features from other third parties like ad networks, to create truthful and clear consumer disclosures. The FTC expects app developers to take responsibility for any third-party data collection and use that its app permits or facilitates.
- Participate in industry initiatives, such as self-regulatory programs, to ensure that they remain current on the latest privacy practices and work to achieve industry practice uniformity.

The FTC Mobile Privacy Report also emphasized that ad networks, analytics companies, and other similar third parties should coordinate and communicate with app developers and mobile platform providers so they can better convey clear and truthful information about their data collection and use practices to consumers. Developers should also execute written contracts with any third parties receiving data from or contributing code to their application. The agreement should clearly describe the technology's tracking and data collection capabilities and establish specific privacy expectations and requirements.

For more on mobile app privacy, see Practice Note, Mobile App Privacy: The Hidden Risks (8-523-6918). For a model mobile app privacy notice, see Standard Documents, Mobile Application Privacy Policy (3-524-0475) and Mobile Application Short-Form Privacy Disclosure (9-525-0329).

TRACKING PRECISE GEOLOCATIONS

Companies may track a person's location using either an IP address, bits of code that ping a device's location, or directly through the device's GPS. Location data is prevalent in today's economy, as mobile apps and websites want to track its consumers' location to deliver targeted advertising and better understand its customer base. Examples of this range from Apple or Android tracking a mobile phone's location and using it to provide directions, estimate travel times, or even predict frequently traveled to destinations at the appropriate times, to apps like Snapchat, Facebook, or FourSquare that track a user's location data using the maps app or "check ins," and then broadcast it to other users.

The FTC's reports consistently recommend that companies collecting, using, or sharing precise geolocation data:

- Provide clear, just-in-time disclosures.
- Obtain the consumer's affirmative express consent.

(FTC Protecting Consumer Privacy Report, pages 59-60; FTC Mobile Privacy Report, pages ii, 15-16, 23-24; FTC Cross-Device Tracking Report, page 15.)

Controversies regarding tracking and sharing geolocations suggest that companies should err on the side of over-disclosure to users and only provide those features on an opt-in basis. They should also leverage privacy by design and default concepts. For example, Snapchat's launch of its 'Snap Maps' feature, which shares a user's location every time the app opens, turned the feature off by default and offered granular location sharing settings.

Most precise geolocation guidance focuses on location in the context of mobile phones (see Mobile Device Tracking), although the guidance applies equally to any technology capable of tracking an individual's precise geolocation.

Industry Self-Regulation and OBA Uses

Several industry organizations provide helpful voluntary guidelines that describe and discuss different precise location use scenarios and recommended requirements, including:

- The Cellular Telecommunications Industry Association (CTIA) Best Practices and Guidelines for Location-Based Services.
- The Groupe Spéciale Mobile Association (GSMA) Privacy Design Guidelines for Mobile Applications.
- Mobile Marketing Association (MMA) Mobile Application Privacy Policy Framework (registration required).

Common themes from the industry guidelines include providing clear, meaningful user notice and obtaining informed consent for all precise location uses. Companies should typically obtain the users express affirmative (opt-in) consent, particularly if the technology stores or shares the location data. However, companies may consider relying on implied consent when the context makes the location use obvious. Companies should also consider storing geolocation data only in password-protected environments and encrypting it in-transit.

In the OBA context, the NAI Code of Conduct and NAI Mobile Code require members to obtain opt-in consent before using precise location data for interest-based or cross-app advertising (see NAI Code of Conduct (2015 Update) § II(C)(1)(d); NAI Mobile Code § II(C)(1)(d)). For more on determining whether location data is precise or imprecise, see Guidance for NAI Members: Determining Whether Location is Imprecise.

GEOFENCING

Other identifying technologies take advantage of unique signals emitted by mobile devices, like the information sent when a mobile device searches for Wi-Fi networks. Businesses can now monitor consumers' movements throughout and around stores by using technologies that pick up signals released by consumers' mobile devices when these are searching and attempting to connect to a Wi-Fi network. This practice of identifying internet enabled devices, like smart phones, when they enter or exit a geographic area is known as geofencing.

Geofencing has a wide range of practical applications. Retailers can leverage geofencing technology to track movement around their physical stores, so they can better understand their customer's behavior or deliver location-based advertisements. Combining geofencing with cross-device tracking also allows companies to deliver OBA advertising as people move around a store or to

a specific location. It can also help companies assess a specific advertising channel's likelihood of success, such as an electronic message, by a tracking recipient's actual purchase behavior.

Geofencing can also raise serious privacy concerns, particularly when used invasively, in unexpected ways, or to track visits to sensitive locations. For example, when Copley Advertising used geofencing technology to tag the smartphones of women entering reproductive health clinics, without the device owner's consent, and then sent anti-abortion advertisements to the tagged devices for one of its clients, the Massachusetts Attorney General's office opened an investigation alleging the actions violated Massachusetts' Consumer Protection Act. The Massachusetts AG was concerned the practice unfairly interfered with a consumer's right to privacy in their medical decisions and conditions and may result in the collection or disclosure of private health or medical facts without the consumer's knowledge or consent.

Copley settled the allegations in April 2017 by entering an Assurance of Discontinuance, where it and its CEO agreed not to use geofencing technology at or near any Massachusetts healthcare facility to infer an individual's health state, medical condition, or medical treatment. For more on Copley's settlement, see Legal Update, Massachusetts AG Settles Geofencing Case with Copley Advertising (w-007-9226).

Industry Self-Regulation

The Future of Privacy Forum issued a Mobile Location Analytics Code of Conduct (FPF Mobile Location Code) to provide companies leveraging geofencing technologies with a self-regulatory framework for using that technology responsibly. The FPF Mobile Location Code recommends that companies:

- Provide clear privacy policies that adequately inform consumers about their collection practices, including any practices that involve appending collected or third-party data to a user profile with a device identifier or hashed device identifier.
- Notify users of any geofencing use that logs information to a unique individual or device using in-store signs or just-in-time notices sent to the mobile device. Include links to the privacy notice.
- Limit collection to the data required for the mobile location analytics.
- Obtain the mobile device user's affirmative consent before:
  - connecting collected mobile location data to personal information or unique device information; or
  - contacting a consumer based on mobile location analytic data.
- Promptly de-identify or de-personalize any personal information temporarily collected, including unique device identifiers, unless the consumer provides affirmative consent to retain it.
- Permit consumers to opt-out in a manner that allows them to maintain full use of the mobile device's features.
- Not use or collect mobile analytic data in a way that may adversely affect the consumer in the areas of:
  - employment eligibility, promotion, or retention;
  - credit eligibility;
  - healthcare treatment or eligibility; or
  - insurance eligibility, pricing, or terms.

These principles, together with additional recommendations on data retention, onward data transfers, and consumer education, provide companies with an important geofencing compliance model.

FACIAL RECOGNITION AND BIOMARKERS

New and innovative facial recognition and biomarker uses, such as gait analysis, have the potential to change dramatically how companies conduct business over the next decade. They also often raise significant individual privacy concerns.

One field experimenting with facial software applications is advertising. Technology advances are starting to make the idea of facial recognition advertisements, first popularized in the science fiction movie, *Minority Report*, into a reality. It may, for example, allow a store to recognize individual customers as they enter, triggering loyalty rewards and tracking the amount of time spent in a particular section, the visit frequency, or the path walked through a store.

As the technology evolves, so do the associated privacy concerns. For example, software may contain errors that can result in inaccurate data and misidentifications.

Facial detection software does not always generate personal information. For example, an app may track facial expressions to identify an anonymous consumer's mood when viewing an advertisement without identifying the person or linking that information to a profile. However, when a company does choose to tie facial features or other biomarkers to an identified person or profile, it must consider the potential privacy impact.

Federal and state law in this area continues to evolve. Some states have already enacted laws governing biometric data collection and use, including:

- Illinois' Biometric Information Privacy Act (BIPA) (740 Ill. Comp. Stat. 14/1 to 14/99).
- Texas' Capture or Use of Biometric Identifier Act (CUBI) (Texas Bus. & Com. Code Ann. § 503.001 (2009)).
- Washington's Biometric Identifiers Act (RCW 19.001.001 to 19.001.004).

Other states are also considering similar legislation. While the existing and proposed state statute requirements and restrictions differ, common themes include:

- Requiring clear consumer notice (transparency).
- Obtaining clear consumer consent, sometimes in writing.
- Allowing consumers to easily opt-out of commercial uses.
- Restrictions on selling, leasing, or otherwise disclosing commercially captured biometric data.

Recent litigation under the Illinois BIPA suggests some facial recognition best practices and potential pitfalls. Under the statute, no private entity can gather or obtain an individual's biometric identifier without first providing specific information in writing and obtaining the person's written consent (740 Ill. Comp. Stat. 14/15(b)). While the statute's "biometric identifiers" definition includes a "scan of hand or face geometry," it also excludes photographs (740 Ill. Comp. Stat. 14/10). This dichotomy led to class action litigation alleging potential BIPA violations from facial recognition technologies that analyze photographs to uniquely identify or tag individuals.

For example, in *In re Facebook Biometric Information Privacy Litigation*, a number of Facebook users alleged that Facebook's collection, retention, and use of information about the geometry of users' faces from their uploaded photographs, without prior written notice or informed consent, violated the BIPA (185 F.Supp.3d 1155 (N.D. Cal. 2016)). Similarly, in *Rivera v. Google Inc.*, a number of Google users alleged that Google's uploading and scanning of their mobile photos to create unique face templates, called "faceprints," for subsequent photo-tagging without their consent also violated the BIPA (238 F.Supp.3d 1088 (N.D. Ill. 2017)).

Both lawsuits survived early motions to dismiss claiming the statute's exclusion of photographs meant the defendants' conduct could not trigger its notice and consent requirements. In each case, however, the court did not consider the photograph itself as the biometric identifier. Instead, it was the defendants' transformation of the photograph into a unique identifier by analyzing and recording the face geometry that qualified as the unique biometric identifier, triggering the statute's protections (*In re Facebook*, 185 F.Supp.3d at 1170; *Rivera*, 238 F.Supp.3d at 1092; see also *Monroy v. Shutterfly*, 2017 WL 4099846 (N.D. Ill 2017)).

While the law in this area continues to develop, companies should provide individuals with clear notice and obtain affirmative consent to gather and use information that may, on its own or after analysis, generate a biometric identifier. For more on biometrics laws and litigation trends, see Practice Note, Biometrics Litigation: An Evolving Landscape (w-001-8264).

FTC Guidance

The FTC's facial recognition guidance also follows the same general themes as the state statutes. Its 2012 report, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies, highlighted the importance of transparency, simplified consumer choice, and incorporating privacy by design practices when considering new facial recognition uses.

Similarly, the FTC's Protecting Consumer Privacy Report discusses how companies leveraging facial recognition technology to create links between offline and online behaviors or compile detailed consumer profiles should both implement privacy by design programs when developing new applications and provide "robust" consumer choice and transparent policies. Specific recommended practices include:

- Adopting the shortest effective retention time for the use purpose. For example, if a digital sign provides targeted advertising based on facial characteristics indicating age or gender, ensure it deletes the consumer's facial profile immediately after the consumer leaves.
- Implementing reasonable security measures.
- Disclosing any practices that link a consumer's facial data to third-party information or information from publicly available sources, including identifying the third-party data source.

(FTC Protecting Consumer Privacy Report, pages 45-46.)

Industry Self-Regulation and OBA Uses

Companies using facial recognition for OBA related activities must consider the industry's self-regulation guides. For example, the NAI Code of Conduct's commentary classifies faceprints as personal information when used to identify a unique, but anonymous, individual (see NAI Code of Conduct (2015 Update), page 12). This differs from the NAI's treatment of a numerical or cookie identifier tied to a unique, but anonymous individual, which it classifies as non-personal information.

NAI members using faceprints for OBA or cross-device advertising must follow the NAI Code's personal information related rules, including:

- Obtaining the person's opt-in consent before merging a faceprint with previously collected non-personal information used for OBA.
- Providing the person with reasonable access to their personal information and any other associated information.

The National Telecommunications & Information Administration (NTIA) released its Privacy Best Practice Recommendations for Commercial Facial Recognition Use in June 2016. Based on the Fair Information Practice Principles, NTIA's guidelines provide a general facial recognition technology roadmap that considers objectives, risks, and individual expectations associated with different technology applications. The guidelines focus on:

- Providing transparency.
- Developing good data management practices.
- Establishing use limitations.
- Enacting security safeguards.
- Maintaining data quality.
- Establishing processes to redress and resolve consumer problems.

Privacy by Design and Impact Assessments

Because of the quickly evolving way companies can use facial recognition in different situations, each unique deployment may generate different privacy issues or concerns. Conducting privacy impact assessments and incorporating privacy by design can help companies catch and address critical issues. For example, a privacy impact assessment may help a company deploying advertising kiosks with cameras avoid placing them in sensitive areas that may generate unnecessary privacy concerns, like bathrooms or health care facility entrances. For more on implementing privacy by design programs, see Practice Note, Developing a Privacy Compliance Program: Box, Privacy by Design (5-617-5067).

DATA BROKERS AND COMBINING DATA FROM MULTIPLE SOURCES

Data brokers collect information about consumers from a wide variety of commercial, government, and other publicly available sources. In developing their products, they not only use the raw data they obtain from these sources, such as a person's name, address, home ownership status, or age, but also certain derived data, which they infer about consumers.

For example, a data broker may infer that an individual with a motorcycle license has an interest in motorcycles or likes risky activities or that a consumer buying more than one Apple laptop has loyalty to that brand. Data brokers use this actual and derived data to create three main kinds of products for clients in a wide variety of industries:

- Marketing products.

- Risk mitigation products.
- People search products.

The FTC issued a report discussing the privacy challenges created by data brokers in May 2014, called Data Brokers: A Call for Transparency and Accountability (FTC Data Broker Report).

Most of the data brokers that sell marketing products provide consumers with limited access to some, but not all, of the actual and derived data the data brokers have about them (FTC Data Broker Report, Page iii). Only some allow consumers to correct their personal information for marketing purposes or allow consumers to opt out of the use of their personal information for marketing purposes.

However, as the FTC notes in its report on data brokers, it is unclear how consumers may learn about these rights, as no centralized portal to learn about access rights and choices provided by data brokers currently exists.

According to the FTC report, a data broker's personal data collection and use practices can potentially lead to several potential consumer harms and risks. For example:

- **Inaccurate or incomplete data** can harm consumers when companies make decisions based the data broker's incorrect information or inferences, such as when an error in a risk mitigation product results in a consumer's inability to conclude a transaction.
- **Lack of transparency** about both the information the data broker collects or shares and the way a company uses that data can harm consumers by preventing them from challenging inaccurate or questionable data, such as when a lender uses a data broker's identity verification product to verify a certain individual's identity before opening a new account. Failing to disclose what caused the lender's decision denies the consumer both the immediate benefit of opening the account and the ability to prevent the problem from recurring.
- **Indefinitely storing personal data** unnecessarily increases the likelihood of harm from potential data breaches, such as when an old address or other outdated information retained provides an identity thief with more authentication credentials. The potential consumer risks may outweigh the benefit of maintaining the information forever.

(FTC Data Broker Report, page ii, v.)

Companies using information purchased from data brokers or append purchased data onto their own customer databases should:

- Disclose the practice in their privacy policies.
- Allow their consumers to view and correct any purchased or appended data related to them.
- Disclose when decisions affecting consumers rely on that appended data or related inferences.
- Incorporate privacy by design practices or conduct privacy impact statements before purchasing or appending data.

Data security represents a second concern with a data broker's transfer and storage of user-related information. Personal information that moves through various servers, which occurs when using the increasingly popular cloud technologies for storage, is more challenging to secure. If not properly configured, others can sometimes see the information while it travels through the cloud. A company using a third party's cloud services also effectively shares information with that cloud provider unless it separately encrypts the data.

DO NOT TRACK REQUESTS

The FTC has endorsed and encouraged the development of a universal "do not track" (DNT) tool for web browsers and mobile devices that provides consumers with a direct way to control monitoring of their online activity (FTC Protecting Consumer Privacy Report, page 52; FTC Mobile Privacy Report, page 20). The FTC Mobile Privacy Report recommends that any DNT system must be, at a minimum:

- Universal.
- Easy to find and use.
- Persistent.
- Effective and enforceable.
- Limit actual data collection, not just its use to serve ads.

(FTC Mobile Privacy Report, page 21.)

However, despite the work of several industry groups and the introduction of browser-based DNT settings, commonly accepted DNT standards do not currently exist.

California also enacted legislation requiring websites or online services collecting personal information from a California resident to disclose how it responds to DNT signals or other consumer choice mechanisms for personal information collected over time and across third-party websites or online services (Cal. Bus. & Prof. Code § 22575(b)(5)-(6)). However, the law does not mandate that websites honor or provide a specific DNT signal response. For more on California's DNT requirements, see Practice Note, California Privacy and Data Security Law: Overview: Privacy Policy Requirements and Do-Not-Track (6-597-4106).

As a best practice, companies should honor a consumer's DNT request whenever it is technically possible and include related disclosures in their privacy policies.

RECOMMENDED BEST PRACTICES FOR US COMPANIES DEPLOYING TRACKING TECHNOLOGIES

Companies deploying tracking technologies should consider the following best practices when designing or reviewing their programs:

- Understand exactly how the tracking technology works, including what data it collects, where it sends data, and the parties that can see the collected data.
- Establish robust privacy by design practices within the business.
- Conduct privacy impact reviews before using or deploying new tracking technologies.
- Ensure all privacy notices or customer-facing statements accurately reflect the tracking technologies used.
- Test all tracking opt-out methods to ensure they work as expected.
- Ensure the instructions for engaging the selected opt-out method accurately describe any dependencies for the feature to work, such as setting the browser to accept third-party cookies if the opt-out method depends on placing a third-party cookie.
- Before using tracking technologies to collect precise geolocations, biometric data or other highly sensitive personal information:

- obtain the person's affirmative opt-in consent; and
- establish data security measures appropriate to the data's sensitivity level.

(See Tracking Precise Geolocations and Facial Recognition and Biomarkers.)

- Companies operating in the healthcare, finance, education, or telecommunications industries should consider the potential impact of sector-specific privacy legislation (see Sector Specific Legislation and Regulatory Provisions).
- If the tracking technology collects or uses personal information:
  - for purposes of making decisions on credit, employment, insurance, housing, and similar eligibility, review the Fair Credit Reporting Act for potential restrictions (see Practice Note, Understanding the Fair Credit Reporting Act (FCRA) (w-001-8260));
  - about students, review FERPA and applicable state student privacy restrictions (see Practice Note, Student Privacy: Education Service Provider Requirements: California Student Privacy Laws (w-001-1128));
  - about children under 13 years old, review the Children's Online Privacy Protection Act for potential restrictions (see Practice Note, Children's Online Privacy: COPPA Compliance (1-555-6526)); or
  - for OBA related activities, join or adhere to the DAA or NAI self-regulatory guidelines (see Online Behavioral Advertising).
- Companies using tracking technologies outside of the US, for example by deploying OBA-related cookies on global websites with non-US visitors, must consider the impact of potentially stricter foreign data privacy laws. The benefits of establishing uniform tracking technology and personal data use policies may lead a company to adopt a stricter procedure or policy approach than US laws require.
- Foreign laws may also apply if companies transfer personal data across borders. For example, if a company's website collects personal data, like an email address, from a visitor located in an EU member state and sends that personal data to a US-based server for storage, it must consider the impact of EU privacy requirements, such as cross-border personal data transfer restrictions.
- Privacy issues, like tracking consumers, are not just legal issues. They also impact customer relations. When deploying tracking technologies, companies should consider industry best practices and customer expectations. Customer relations may require the company to go beyond what US law requires.

TRACKING-RELATED FEDERAL AND STATE ENFORCEMENT ACTIONS

VIZIO, INC.

The FTC filed a complaint against TV manufacturer Vizio, Inc., charging that it engaged in deceptive practices by installing tracking software on its products without alerting customers. The software captured viewing habits, combined it with consumers' personal information on home ownership and education. Vizio then sold that combined data to third parties. Importantly, Vizio tracked its consumers' viewing habits without obtaining consent. In a 2017 settlement with multiple regulatory agencies, Vizio agreed to pay $2.2 million to the FTC and the New Jersey Division of Consumer Affairs and promptly obtain express consent for its data collection practices. Vizio also agreed to delete data collected without consent and implement a comprehensive data privacy program.

The Vizio consent decree is a reminder that companies need to obtain consent before tracking sensitive personal information, such as unique viewing data, and using or sharing it for advertising. For more on Vizio's settlement, see Legal Update, FTC and New Jersey Attorney General Fine Vizio, Inc. $2.2 Million Over Data Collection From Smart TVs (w-005-8525).

TURN, INC.

In the Matter of Turn Inc., the FTC claimed that Turn misled its consumers by stating in its privacy policy that it intended to honor opt-out requests and allow consumers to block tracking cookies. However, the company ignored those requests and allowed clients to use targeted advertising against the consumers. Following a consent decree, Turn agreed to provide an effective opt-out mechanism and prominently link to it. As this case demonstrates, the FTC enforces published privacy policies and companies must follow their own words closely. For more on Turn's settlement, see Legal Update, FTC Settles Charges with Digital Advertisement Company for Deceptively Tracking Consumers (w-005-1093).

GOOGLE'S 2012 FTC SAFARI BROWSER COOKIE SETTLEMENT

In August 2012, Google Inc. agreed to pay a record $22.5 million civil penalty to settle FTC charges that it misrepresented how to block or opt out of tracking cookies and prevent behaviorally targeted ads to users of Apple Inc.'s Safari Internet browser. According to the FTC's complaint, Google specifically told Safari users that Safari's default settings opted them out of Google's tracking cookies. Google's privacy notice also represented that it was a member of the Network Advertising Initiative's industry group, which requires members to adhere to its self-regulatory code of conduct, including disclosure of data collection and use practices. The FTC alleged that Google's use of Safari cookies without informing its users violated the NAI code, and that Google's misrepresentations violated a settlement it reached with the FTC in October 2011, which barred Google from, among other things, misrepresenting the extent to which consumers can exercise control over the collection of their data. For more on Google's settlement, see Legal Update, FTC Settles Privacy Complaints Against Google and Facebook (4-520-8521).

NY AG'S COPPA SETTLEMENTS WITH VARIOUS TOY MANUFACTURERS

For two years, the New York Attorney General's office secretly investigated the privacy practices of toy manufacturers Mattel, Hasbro, Viacom, and Jumpstart. Called Operation Child Tracker, the investigation revealed that the companies tracked online activity of children under the age of 13, in violation of

the Children's Online Privacy Protection Act (COPPA). COPPA prevents anyone from collecting personal information on children under 13 without express parental consent.

The violations primarily stemmed from improperly configured or deployed third-party advertising trackers. Mattel, Hasbro, Viacom, and Jumpstart agreed to pay $835,000 in fines and adopt new procedures that prevent unexpected third-party tracking of children to settle the AG office's complaint. While the fine is minor compared to the companies' annual revenue, which stretches into the billions of dollars, it illustrates the importance of understanding the impact of permitting third-party tracking technology to operate within a company's website or product and respecting the privacy of children. For more on the COPPA settlements, see Legal Update, NY Attorney General Announces COPPA Violation Settlements with Four Companies (w-003-4757).

NY AG'S UBER SETTLEMENT

The New York Attorney General's office also reached a settlement with Uber after an investigation revealed that employees regularly accessed rider data and tracked riders in real-time using a special Uber tool called "God View." In the settlement, Uber agreed to:

- Encrypt and password-protect its rider location data.
- Limit rider information access to designated individuals with a legitimate need for it.
- Regularly review privacy and access controls.
- Explain its rider geo-location information policies in a separate privacy policy section.

Cases of employees accessing personal information without authorization can occur at any company. In response, companies must secure their data sources and ensure that only those employees with appropriate user privileges can access them. For more on Uber's settlement, see Legal Update, Uber Settles NY AG Investigations Into Data Breach and Privacy Practices (w-001-3143).

COPLEY ADVERTISING'S GEOFENCING SETTLEMENT

In 2015, Copley Advertising, on behalf an advertising client, deployed geofencing technology to identify "abortion-minded" women by tagging the smartphones of women entering reproductive health clinics, without the device owner's consent. Copley then sent anti-abortion advertisements to the tagged devices. The Massachusetts Attorney General's office opened an investigation alleging that Copley's actions violated Massachusetts' Consumer Protection Act by unfairly interfering with a consumer's right to privacy in their medical decisions and conditions. It was also concerned that the geofencing practice may result in the collection or disclosure of private health or medical facts without the consumer's knowledge or consent.

Copley settled the allegations in April 2017 by entering an Assurance of Discontinuance, where it and its CEO agreed not to use geofencing technology at or near any Massachusetts healthcare facility to infer an individual's health state, medical condition, or medical treatment.

The settlement appears to be the first settled case asserting a consumer protection law against geofencing. For more on Copley's settlement, see Legal Update, Massachusetts AG Settles Geofencing Case with Copley Advertising (w-007-9226).

VERIZON WIRELESS FCC SUPERCOOKIE SETTLEMENT

In mid-2016, Verizon Wireless agreed to pay a $1.35 million fine to the FCC under a three-year consent decree. The FCC's initial complaint alleged that Verizon inserted unique identifier headers (UIDH), known as supercookies, into its mobile customers' internet traffic to track unique web browsing activity and create user profiles for behavioral advertising, without providing notice. Unlike typical internet cookies, users were unable to delete or use browser preferences to reject these supercookies. Verizon also allowed third-party advertisers to access its customer's web browsing information regularly and, in at least one case, use the supercookie technology to restore third-party internet-tracking cookies that users intentionally deleted. The FCC alleged these actions violated the Communications Act and the Open Internet Transparency Rule.

In addition to the fine, the FCC's consent decree required Verizon to obtain their users' express opt-in consent before sharing supercookie information with third parties and to allow users to opt out of supercookie use. For more on the settlement, see Legal Update, Verizon Wireless Settles FCC Supercookie Investigation for $1.35 Million (w-001-5026).

09-17