
Hughes Hubbard & Reed

顔認識技術：民間使用に対する拡大する規制

Client Advisories

Hughes Hubbard & Reed LLP • A New York Limited Liability Partnership
One Battery Park Plaza • New York, New York 10004-1482 • +1 (212) 837-6000

Attorney advertising. Readers are advised that prior results do not guarantee a similar outcome. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. For information regarding the selection process of awards, please visit <https://www.hugheshubbard.com/legal-notices-methodologies>.

携帯電話のロック解除からソーシャルメディアにおける顔のマッピングに至るまで、顔認識技術（Facial Recognition Technology「FRT」）は急速に我々の生活の一部になってきています。この新技術を用いる企業は法規制に注意深く従う必要があり、これを怠った場合には高額な制裁金を課されたり、クラス・アクションを提起されたりすることになります。今年の初め、フェイスブック社が5.5億ドルでクラス・アクションについて和解するとのニュースがありましたが、裁判所により、この金額は法に定められた損害の最高額の1.25%に過ぎないと指摘されました。本アラートでは、FRT規制に関する施行済み及び審議中の法律について説明します。

顔認識技術の隆盛

企業はFRTを様々な用途に用いています。携帯電話は、所有者の顔を認識することでロックを解除します。オンライン販売業者その他の企業は、FRTを注文及び支払い用のアプリに用いています。消費者は、FRTを用いて化粧品及び眼鏡の試用をシミュレーションすることができます。路面店は、FRTを用いて万引きに対処しています。レストランは、顧客の好みを記録したり、接客係の対応を管理したりするためにFRTを利用しようとしています。新型コロナウイルス対応として、企業は体温と同時に顔の形状を捉える技術を用いています。

民間におけるFRTの使用は将来にわたり引き続き拡大していくと思われます。FRTはオフィス及び施設への安全なアクセスを実現するでしょう。自動車は、我々の顔を認識した上で、解錠し、自動的にシート、ミラーその他のコントロールを、我々の好みの設定に自動的に調整するでしょう。ダッシュボードのカメラは、運転手が疲れていないかをチェックするようになるかもしれません。航空会社は、チェックイン及び搭乗の際にFRTを用いて乗客の確認をし、またホテル及びレンタカー会社は、FRTを用いて速やかなチェックインを行い、顧客対応を個別化するでしょう。ヘルスケア業界は既にオンライン診療を開始し、FRTを用いて顧客登録を円滑化し、保険詐欺を防止し、また一部の病気の診断を行うことを目指しています。

生体特定要素に特に着目した州法

指紋、網膜スキャン及びFRTなどの生体特定要素（biometric identifiers）の使用増加に対応し、多くの州が法律を制定しました。イリノイ州、テキサス州及びワシントン州は、生体特定要素に特に着目した法律を有しています。イリノイ

州の生体情報プライバシー法（Biometric Information Privacy Act (740 ILCS 14/)「BIPA」）は、「生体特定要素」に「顔の形状」が含まれるとして、顔データの収集につき事前の同意を必要とし、第三者への生体データの販売を制限しています。BIPAは私人が訴訟を提起する権利を付与していることで有名であり、これをもとに何百ものクラス・アクションが提起されています。

テキサス州の生体特定要素の捕捉又は使用に関する法律（Statute on the Capture or Use of Biometric Identifier (Texas Bus. & Com. Code Ann. Sec. 503.001)）はBIPAに類似しています。同法もまた「生体特定要素」に「顔の形状」が含まれると定義し、同意が必要とされ、また第三者への販売が制限されています。もっとも、同法は私人が訴訟を提起する権利を付与していません。

ワシントン州の生体特定要素関連法（Act Relating to Biometric Identifiers (RCW 19.375.010, et seq.)) はBIPAと大きく異なっています。特に、同法は「生体特定要素」から「物理的若しくはデジタルの写真、ビデオ及び音声記録、又はこれらから取得されたデータ」を除外しており、また私人が訴訟を提起する権利を与えていません。

データ保護及びプライバシーに関する州法

カリフォルニアは、カリフォルニア消費者プライバシー保護法（California Consumer Privacy Act (Sec. 1798.100, et seq.)「CCPA」）により生体データを保護しています。CCPAはカリフォルニア州の消費者に対し、「生体情報（biometric information）」を含む個人情報に対する強力なデータ・プライバシー権及びコントロールを付与しています。かかる生体情報には、例えば顔認識用のデータを抽出できる顔イメージが含まれます。企業は顔データを含む「個人情報」収集につき事前の通知をしなければならず、また当該情報の保護のための合理的な措置を行う必要があります。以前アラートでお伝えしたとおり、CCPAは私人が訴訟を提起する権利を付与しており、既に消費者によりいくつかのクラス・アクションが提起されています。

データ漏洩通知に関する州法

ニューヨーク州は、ハッキング防止及び電子データ保護向上法（Stop Hacks and Improve Electronic Data Security Act (Senate Bill S5575B, enacted)「SHIELD法」）により生体データを保護しています。SHIELD法は同州のデータ漏洩通知に関する法律を改正し、種々の生体データ保護を追加しました。同法は、「個人情報」の定義を拡大して生体データもこれに含まれるとし、また漏洩（breach）の定義及び同法の地理的管轄も拡大しました。同法はまた、企業に対し個人情報保護のための合理的な措置を採ることを要求しています。

また、様々な州が生体データを対象に含むデータ漏洩通知法を有しています。かかる州法には、たとえば、アーカンソー州の個人情報保護法（Personal Information Protection Act (A.C.A. Sec. 4-110-101, et seq.))、ルイジアナ州のデータ漏洩セキュリティ通知法（Louisiana’s Data Breach Security Notification Law (La. Rev. Stat. 51:3071, et seq.))、メリーランド州の個人情報保護法（Personal Information Protection Act (Md. Code Ann. Comm. Law 14-3501, et seq.))、オレゴン州の消費者情報保護法（Consumer Information Protection Act (ORS 646A.600, et seq.))、バーモント州のセキュリティ侵害通知法（Security Breach Notice Act (9 V.S.A. Secs. 2430 & 2435))、コロラド州の消費者データ・プライバシー保護法（Protections for Consumer Data Privacy Act (Colo. Rev. Stat. Sec. 6-1-713, et seq.))、及びノースカロライナ州の個人特定情報窃盗防止法（Identity Theft Protection Act (N.C. Gen. Stat. Sec. 75-61, et seq.))があります。

審議中の州法

本アラートを作成している時点で、他の州でも顔データを含む生体特定要素を保護する法案が審議されていました。現在、ハワイ州（Senate Bill No. 418）、マサチューセッツ州（Bill S. 120）及びアリゾナ州（HB 2729）で、生体情報の収集に事前の通知を必要とし、消費者に対し自らのデータを削除させる権利を与える法案が審議されています。ハワイ州及びアリゾナ州の法案はまた、消費者に対しデータの販売から離脱する権利を与え、またマサチューセッツ州の法案は、消費者に対し、第三者に対するいかなる開示からも離脱する権利を与えています。

審議中の連邦法

米国には、データ保護に関する連邦法はありません。連邦取引委員会（Federal Trade Commission「FTC」）が消費者のプライバシーを不公正又は欺罔的な行為又は慣行の取締りとして保護しており、特定の産業毎の種々の法律により個人情報保護されています。例えば、グラム・リーチ・ブライリー法（Gramm-Leach-Bliley Act）は金融機関による「非公開の個人情報」の使用を制限しており、医療保険の相互運用性及び説明責任に関する法律（Health Insurance Portability and Accountability Act）は対象機関に対し健康情報の保護を義務付けています。しかしながら、民間によるFRTの使用を特別に規制する連邦法は存在しません。

連邦議会は、現在、プライバシーに関する多くの法案を審議しており、少なくともそのうち2つは、仮に成立すれば、民間によるFRTの使用に直接影響を与えます。1つ目の法案はSenate Bill S. 847（2019年商業用顔認識プライバシー法：Commercial Facial Recognition Privacy Act of 2019）であり、これによると、顔データの収集及び使用について積極的な同意が必要であるとされています。2つ目の法案はSenate Bill S. 3456（2020年消費者データ・プライバシー法：Consumer Data Privacy and Security Act of 2020）であり、これによると、生体データ及び顔データを含む「機密個人情報（sensitive personal data）」の収集及び加工につき、明示かつ積極的な同意が必要とされています。これらの法案はともに、FTCに執行の責任を負わせていますが、同時に各州の司法長官による訴訟提起を許容しています。2つ目の法案では、FTCに対し、データ・プライバシー及びセキュリティに関する法の執行のため、440人以上の増員を義務付けています。

結論

クラス・アクションが増加し、また当局による規制執行が強化されていることから、FRTを使用する企業は成立済み及び審議中の法律を注意深く検討する必要があります。州により異なりますが、現行の法規制及びベスト・プラクティスには、以下のものが含まれます。

- (1) 顔イメージの収集対象となっている消費者に対し通知し、それがどのように保管及び使用されているかを説明する。
- (2) 顔イメージ収集の前に同意を得る。
- (3) 合理的なセキュリティ対策及びプラクティスを実施する。
- (4) データ漏洩が起きた際に通知を行う。
- (5) 顔データの販売を禁止するポリシーを策定する。
- (6) ベンダーに対し、法遵守、セキュリティ侵害の際の速やかな通知、及びコンプライアンス確保のための定期的な監査の受入れを要求する。

上記の各点について追加の情報又はアドバイスが必要な場合には、以下のヒューズ・ハバードの弁護士にご連絡ください。

Seth D. Rothman | Partner

Hughes Hubbard & Reed LLP

One Battery Park Plaza | New York, NY 10004-1482

Office +1 (212) 837-6872 | Cell +1 (917) 697-8093

seth.rothman@hugheshubbard.com | [bio](#)

Rita Haeusler | Partner

Hughes Hubbard & Reed LLP

1999 Avenue of the Stars, 9th Floor | Los Angeles, CA 90067-4620

Office +1 (213) 613-2896 | Cell +1 (917) 544-3587 | Fax +1 (213) 613-2895

rita.haeusler@hugheshubbard.com | [bio](#)

Paul Marston | Counsel

Hughes Hubbard & Reed LLP

Kojimachi Place, 9th Floor, 2-3 Kojimachi | Chiyoda-ku, Tokyo 102-0083, Japan

Office +81-3-6272-5831 | Cell +81-80-8432-3497

paul.marston@hugheshubbard.com | [bio](#)

Shigeki Obi | Associate

Hughes Hubbard & Reed LLP

One Battery Park Plaza | New York, NY 10004-1482

Office +1 (212) 837-6106 | Cell +1 (347) 446-7428

shigeki.obi@hugheshubbard.com

Related People



Seth D. Rothman



Rita M. Haeusler



Paul Marston



Shigeki Obi

Related Areas of Focus

Data Privacy & Cybersecurity

English version