NII Special
2

パーソナルデータの制御権を自らの手に！

恣意的な顔認識へ議論を投げかける「プライバシーバイザー」

ビッグデータ収集と解析技術の発展により、パーソナルデータが予想もつかない目的に利用される危険性が指摘されるようになった。SNSに登録・投稿されるコンテンツから、写真に写った人物の氏名や住所などの個人情報が、本人の意思とは無関係に丸裸にされてしまう事態が現実のものになったのだ。サイバー空間のパーソナルデータは本人の手で制御できないものなのか？ NIIの越前功教授が開発する顔検出防止ツール「プライバシーバイザー」が、ビッグデータ活用とプライバシー保護の議論に新たな一石を投じている。

顔認識の問題点

カメラ付き携帯電話やスマートフォンの普及とSNSの利用拡大に伴い、街角や施設内のスナップ写真が気軽にインターネットに公開されることが多くなっている。被撮影者にはその許可を得ていたとしても、背後にたまたま映り込んだ人は、自分の写真が公開されることなど想像してもいないに違いない。ところが現在の顔認識技術によれば、その写真に映り込んだ顔の特徴から、同一人物を探し出すことが簡単にできてしまう。さらに、写真に付帯する情報から、日時と位置情報まで公開されてしまうこともある。人物が同定できれば、インターネット上にある数々の情報源から関連する情報を検索・収集することは難しくないだろう。つまり、たった1枚の写真への映り込みから、自分がいつ、どこで、何をしていたかが見知らぬ誰かの知るところとなり、リンクをたどればどんな仕事をし、どんな仲間がいるのかといった情報まであからさまになってしまうのだ。

さらにGoogle Glassに代表されるカメラ搭載ウェアラブルデバイスの実用化が目前になっており、こうしたデバイスを通して見た人物のパーソナルデータが、その場でリアルタイムにわかる時代がすぐそこまで来ている。

「自分の情報がサイバー空間に拡散し、商用にも利用されてしまう現実に対して、個人が自分自身のプライバシーを守るために何ができるかを考えてほしい」と、NIIの越前功教授は語る。「例えば、米カーネギーメロン大学が匿名で写真撮影に同意した人の顔写真をもとにFacebookに照合して人物同定ができるかを実験したところ、被験者の1/3の同定に成功、個人的な興味関心事や社会保障番号の一部も判明してしまいました。顔写真だけでプライバシーが暴かれる時代がすでに到来しているのです」※

越前 功
Isao Echizen
国立情報学研究所
コンテンツ科学研究系 教授
総合研究大学院大学 複合科学研究科
情報学専攻 教授

顔検出を無効化する「プライバシーバイザー」

ビッグデータが活用可能な時代だからこそ生じているプライバシー侵害への懸念から、越前教授が急ピッチで研究・開発を続けているのが「プライバシーバイザー」だ。「プライバシーバイザーは、パーソナルデータである『顔』画像を恣意的に利用されないように自衛するための試みです。情報を収集する側の仕組みがどのようなものであれ、被撮影者の側でこれを装着することにより、顔認識の前処理である顔検出を無効化して、プライバシー侵害

を防ぐことができます」と越前氏は言う。

いまや一般的なデジタルカメラでも、映像の中から人の顔だけを検出する技術が搭載されている。代表的な顔検出手法としてViola-Jones法が採用されていて、顔の特徴量として主に目の周辺と鼻筋、および鼻の周囲の輝度（明暗）の差を抽出し、蓄積・学習した顔の特徴データと照合して顔を検知する。

この手法はかなり精度がよく、越前教授の実験では22m離れた場所からの撮影でも顔検出ができるばかりか、デザインの異なる5種類のサングラスで変装してみても、顔が正しく検出できたという。この顔検出を失敗させるための対策として、これまでは特殊な顔面着色や髪型、あるいは顔面を蔽うマスクの着用が提案されてきたが、現実世界の対面コミュニケーションに支障をきたすという弱点があった。もっと自然に利用できる顔検出防止ツールとして開発されたのが、ゴーグル型のプライバシーバイザーだ。

越前教授は目の周辺領域を蔽う形状のゴーグルに11個の近赤外LEDを取り付け、顔検出されたくない時にLEDを点灯できるようにした。人間の可視域を超える波長の光なので、点灯状態でも対面する人には光は見えないが、民生用のカメラは赤外領域まで感知するため、LEDの光はノイズとして映る。その結果、目の周囲の輝度差が検出できなくなり、顔検出に失敗するというのがプライバシーバイザーの仕組みだ。

カメラの前に10人の被験者を並べて撮影した実験によると、バイザーを装着しない場合には、20m離れたところの被験者のうち7～8人の顔検出に成功した。バイザーを装着しただけでは顔検出率にあまり差はなかったが、LEDを点灯した場合には、22m以内にいる人物は誰ひとり顔検出ができなかった。

電源不要でファッショナブルな新プライバシーバイザー

ただし、この試作品ではLEDを点灯するために電池を要するところに難があった。また、プロ用のカメラでは赤外領域を感知しないので効果がない。そこで越前教授は昨年末から眼鏡製造で世界的に有名な福井県鯖江市の眼鏡メーカー数社と共同で、LED不要の新しいプライバシーバイザーの開発を進めている。

プライバシーバイザーのプロトタイプ

新プライバシーバイザーは、顔検出器が暗いと判断する目の周囲などの窪んだ領域に可視光を反射する素材を採用し、逆に顔検出器が明るいと判断する鼻上部などの出っ張った領域には可視光を吸収する素材を採用。試作品は白を基調に、細かいドットや文様を透明部分に散りばめた。これなら、サングラスのように持ち歩きにも装着にも比較的違和感や負担感は少なそうだ。デザイン上の工夫も加えながら、年内にはプロトタイプ出荷を目指しているという。

情報の利活用とプライバシー保護のバランスが重要

一方、懸念されるのは、プライバシーバイザーが犯罪を助長しはしないかという点だ。

「例えば空港の監視カメラでテロリストを発見するといった目的で顔認識が使われていますが、そうした場所でのプライバシーバイザーの着用は禁止するなど、制度面での対策が必要でしょう。公益とプライバシー保護のバランスが大事です」と越前教授。プライバシーバイザーは、こうした課題への問題提起でもあるのだ。

さらに越前教授は、プライバシーバイザーの着用が個人画像の利用を拒否するサインとなる可能性を指摘する。人の装着物（アクセサリ、バッジなど）によって、自分のパーソナルデータの利用範囲を表明し、その条件に基づいてデータの利活用が図れるようにする仕組みの提案も視野に入れているのである。

ビッグデータ時代の今日、自分のパーソナルデータの何を守り、何を公開すればリスクを最小にして最大の利益が得られるのか、自衛方法も含めてよく考える必要がありそうだ。

（取材・文＝土肥正弘）

※Facebookの顔認識機能については、2012年に欧州連合（EU）からの要請を受けて、欧州に限って提供しないことが決まった。Google Glassも顔認識機能は搭載しないことを表明している。しかし、このような技術が実用レベルにある以上、両社が提供しなくても新たなサービス業者やアプリケーション開発業者が開発、提供しないとは言い切れない。