

2016/11/17

SOFITC 判例ゼミ 2016 (第5回)

ディスカッションポイント

1. 本件事案について

- 本件事案は、幅広く報道され世間の注目を集めました。セーフハーバーを利用して EU から米国に個人データを転送している日本企業は多くはなく、日本企業への影響は限定的と評価されています。実際に、この件から企業法務実務上何らかの影響がありましたか。

【ゼミ生・講師からのコメント】

→ 特段の実務上の影響はなし。

2. 個人としてのプライバシーの問題

※本件では、2013 年のスノーデン事件により NSA 等の米国政府機関が Facebook 等のデータを監視していたことが事案の発端となりました。個人として、プライバシーの保護と利用のバランスの問題についてどのような感覚を持ちますか。

(1) Pokémon Go プライバシーポリシー

<https://www.nianticlabs.com/privacy/pokemongo/ja>

Niantic による情報の収集・利用

「2. 情報の収集及び使用

a. お客様（又はそのお子様）から収集又は受領した情報
(略)

i. アカウント情報

当社は、ゲームプレイ中及びお客様（又はそのお子様）が当社でのアカウント（以下「本アカウント」といいます。）を作成登録するときに、**お客様（又はそのお子様）を特定又は識別しうる一定の情報（以下「個人情報」といいます。）を収集します。**具体的には、お客様が本アカウントを作成登録する場合、事前にグーグル、Pokémon トレーナークラブ（以下「PTC」といいます。）又はフェイスブックのいずれかのアカウントを保有している必要があるため、当社は、お客様のグーグル、PTC 又はフェイスブックにおけるプライバシー設定により当社からのアクセスが許容される個人情報（例えば、お客様のグーグル電子メールアドレス、PTC 登録電子メールアドレス、及びフェイスブック登録電子メ

ールアドレス) を収集します。

(略)

e.位置情報

本アプリは、位置情報を基にしたゲームです。当社は、お客様（又はそのお子様）が本アプリを利用して、お客様（又はそのお子様）の機器のモバイルオペレーティングシステムを通じて利用できる位置情報サービス（携帯電話基地局による三角測量、Wi-Fi による三角測量又は GPS を利用するもの）を使用するゲーム上のアクションを行った際に、お客様（又はそのお子様）の位置情報を収集及び保存します。お客様（又はそのお子様）が本アプリを利用した場合にお客様（又はそのお子様）の機器の位置情報が当社に送信されること、また、かかる位置情報の一部及びお客様（又はそのお子様）のユーザー名が本アプリを通じて共有される可能性があることをご理解のうえご了承ください。」

「3. 当社が第三者と共有する情報

a.株式会社ポケモン(以下「TPC」といいます。)及び TPCI と共有する情報

お客様が本アカウントを作成登録し、本サービスの運用又は開発においてバグ、エラーその他事故や問題が発見された場合で、当該問題を調査し、原因を突き止め、修正し、及び解決するために TPC 及び TPCI と協力することが必要なときは、当社は、お客様（又はそのお子様）の個人情報を TPC 及び TPCI と共有できるものとしします。(略)

c.第三者と共有する情報

当社は、調査及び分析、人口動態（デモグラフィック）のプロファイリング、並びにその他の類似の目的のために、集約された情報及び個人を特定できない形式の情報を第三者と共有できるものとしします。かかる情報にはお客様（又はそのお子様）の個人情報は含まれません。」

- 上記プライバシーポリシーによると、サービス提供者の Niantic は利用者の個人情報、位置情報を詳細に把握できるとされています。ゲームが楽しいのであれば、これら情報の提供は差し支えないと感じますか？（「a. お客様（又はそのお子様）から収集又は受領した情報」「i. アカウント情報」「e.位置情報」）
- さらに、上記プライバシーポリシーによると、Niantic は、「調査及び分析、人口動態（デモグラフィック）のプロファイリング、並びにその他の類似の目的のため」に、位置情報等を第三者と共有できるものとされています。かかる情報

には個人情報に含まれないとされていますが、そうであれば自身の情報が第三者と共有されることについて差し支えないと感じますか？（c.第三者と共有する情報）

【ゼミ生・講師からのコメント】

- 「ゲームの面白さが勝れば、個人情報が収集されても差支えない。」
- 「蓄積された情報から価値が生まれ、その結果無償でゲームが利用できるという便益が得られている。」
- 「ゲーム会社の従業員が信用できるとは限らず、個人情報の提供には抵抗を感じる。」
- 「自身の個人情報を提供することは差支えないが、子供の個人情報の提供は避けたい。」
- 「GPS 情報は端末側で ON/OFF ができ、利用者側でも自身の情報が提供されることをコントロールできる。」
- 「属性情報なら提供して差支えないという意見もあるが、例えば『この地域に 20 代の女性が多い』という属性情報が悪用されるケースもあるため、属性情報にも危険性はあるといえるのではないか。」

(2) Yahoo メール監視問題

<http://jp.reuters.com/article/yahoo-nsa-idJPKCN12500Z>

米ヤフー(YHOO.O)が昨年、米情報機関からの要請を受けてヤフーメールのユーザーのすべての受信メールをスキャンしていたことが、関係筋の話から明らかになった。

ヤフーの元社員 2 人と別の関係筋によると、ヤフーは米国家安全保障局(NSA)もしくは連邦捜査局(FBI)の要請に基づき、数億件のヤフーメールのアカウントをスキャンし、情報機関が求めていた特定の情報をサーチしていた。

情報機関はヤフーに対し特定の文字をサーチするよう要請していたが、どのような情報を求めていたのかは明らかになっていない。関係筋によると、メールもしくは添付ファイルに記載されたフレーズを求めていた可能性がある。

ロイターは、ヤフーが情報機関にデータを手渡したのであれば、それがどのような内容だったのか特定できていない。また、情報機関がヤフー以外の企業に同様の要請を行っていたのかも不明。

- 仮に問題となった米国の Yahoo mail を利用していたとした場合、このニュースを聞いても Yahoo mail の利用を続けますか？
- Gmail 等でも同様に米国政府によってメールの監視が行われている可能性がある

ると指摘されています。このニュースを聞いても、Gmail 等の米国企業によるサービスを使い続けたいと思いますか、それとも国内業者によるメールサービスに移行しますか？

- 日本では、当局によるメールの閲覧には捜索差押え令状が必要であり、特定の事件の捜査目的でしかメールの閲覧はできないとされています。日本でも犯罪予防のためにメールの監視を認めるようにすべきだと思いますか？

(3) 警察による位置情報の取得

<http://bylines.news.yahoo.co.jp/maedatsunehiko/20160525-00058016/>

捜査当局は、裁判官から検証許可状を取った上で、携帯電話会社が把握している GPS の位置情報を入手している。これに加えて、従前の総務省の個人情報保護ガイドラインが「当該位置情報が取得されていることを利用者が知ることができるときであって、裁判官の発付した令状に従うときに限り、当該位置情報を取得するものとする」と規定していたことから、従前携帯電話各社は、これまで端末のバイブ機能でスマホを振動させたり、通知音を出した上で、画面にも「位置情報が検索されようとしています」といった表示を出し、ユーザーに知らせてきた。

ところが、今年 6 月に総務省のガイドラインは改定されて利用者への通知を求める規定が削除され、携帯電話各社はこれに対応して通知を不要とする対応を行っている。

- 携帯電話の GPS 情報は通知なく捜査に利用されることとなりましたが、それでも携帯電話の GPS を使い続けますか？位置情報取得の場合の事前の通知は必要だと思いますか？事後的にであっても通知をさせるべきですか？
- 位置情報は警察の捜査に有効活用されており、例えば今年 5 月の沖縄県うるま市における女性殺人事件等において位置情報が犯人逮捕につながったことが報道されています。警察が位置情報を捜査目的に収集・利用することに問題はありますか？むしろ、令状を必要とせず犯罪予防目的等も含め幅広く位置情報を取得できるようにすべきですか？

【ゼミ生・講師からのコメント[※(2),(3)まとめて]

- 「犯罪防止・テロ対策等の安全のためであれば個人情報の取得も止むを得ない。」
- 「日本では通信の秘密が憲法上で保障されているため、日本ではプロバイダによるメールの監視はありえない。」
- 「日本のプロバイダの方が信用できるので、日本のプロバイダが提供するメールを利用したい。」

- 「刑事事件のみならず、民事裁判でも文書送付嘱託、文書提出命令との関連でどこまで情報収集を認めるかが問題となる。」
- 「メールのみならず、クレジットカードの購入履歴、通販サイトの購入履歴も収集・蓄積されており、企業・当局による取得・利用の対象になりうる。」

3. 企業としてのプライバシー関連問題における意思決定

※プライバシー問題に関しては、様々な利益考量が必要となり、企業として難しい判断を迫られる状況が少なくないと想定されます。そのような状況において、企業としてどのように意思決定を行いますか。

(1) 社用メール等のモニタリング

<http://www.nikkei.com/article/DGXMZO96091320U6A110C100000/>

今年1月12日、欧州人権裁判所が、ルーマニアの企業が従業員のヤフーメッセージャーのアカウントを監視したことは、従業員のプライバシー侵害にはあたらないとの判決を下したとの報道がされました。報道によると、この男性の雇用主は2007年、同氏が勤務時間中に職場のコンピューターで兄弟や婚約者とやりとりしたメッセージの45ページに及ぶ写しを突きつけて男性を解雇した。顧客と瞬時にチャットでやりとりするよう会社から言われ、男性はヤフーアカウントを設定したが、そのアカウントを個人的に使用することは禁じられており、男性は、会社がプライバシーに関する人権を侵害したとして不服を申し立てたが、欧州人権裁判所は「雇用主が就業時間中に従業員がしかるべき業務を遂行しているか検証したいと考えることは不当ではない」と結論づけたとのことでした。

この点、日本では、東京地判平成13年12月3日（F社Z事業部事件）が「社内ネットワークシステムにおける労働者の電子メールの監視については、監視の目的、手段及びその態様を総合考慮し、監視される側に生じた不利益とを比較衡量の上、社会通念上相当な範囲を逸脱した監視がなされた場合に限りプライバシーの侵害に該当する」として、社員によるメールの私的利用を監視する目的でのモニタリングは許容されると判断しています。

- 皆さんの会社では、社用メール等について、どの程度のチェックがされていますか？以下の点についてはいかがでしょうか？
 - ①社用メールの内容のチェック
 - ②ネット閲覧履歴のチェック
 - ③私用メール（Gmail等）、メッセージャー等の通信内容のチェック
 - ④ローカル・サーバー上に保存しているデータのチェック

- 監視の目的（企業秩序違反の調査、セキュリティ目的等）、監視者（部門の上長、IT部門）についてはどのような規程・体制となっていますか？
- 社用ネットワークであっても、プライバシーについて保護されるべきと考えますか？会社側によるモニタリングに限界はあると考えますか？

【ゼミ生・講師からのコメント】

- ゼミ生の勤める殆どの企業で社用メール等のモニタリングを実施。目的は、職務専念のチェック、セキュリティ等。
- 「会社による監視の必要性は理解するが、あまりがんにがらめにされるのも息苦しい。」
- 「会社の業務とは直接関係のない活動から新たなアイデアが生まれることもあるのではないか。」
- 「セキュリティに関しては、データ持ち出しを企むものはそもそも社内メール使わないであろうから、監視をしてもあまり意味がないのではないか。」

(2) 捜査当局によりメールの提出を命じられる場合（資料 5：NY Times 記事、資料 6：毎日新聞記事）

http://www.nytimes.com/2016/07/15/technology/microsoft-wins-appeal-on-overs-eas-data-searches.html?_r=0

<http://mainichi.jp/articles/20160318/k00/00m/040/142000c>

今年 7 月 14 日、マイクロソフト社が、2013 年にアイルランドのデータセンターに保存されている顧客のメールを提出するようニューヨーク連邦地裁から捜索令状を発令された件について、3 年間におよぶ法廷闘争の末連邦第 2 巡回区控訴裁判所によって捜索令状を取り消す決定を得たことが報道されました。

他方、日本でも、捜査機関が押収したパソコンから Google のサーバーに接続してメールを入手したことが違法であると裁判所によって指摘された事例が報道されています。なお、この事例はサーバーへの接続が差し押さえ後に行われたことが違法と判断された根拠になっていますが、サイバー犯罪条約 32 条が、「締約国は、他の締約国の許可なしに、次のことを行うことができる。(略) b 自国の領域内にあるコンピュータ・システムを通じて、他の締約国に所在する蔵置されたコンピュータ・データにアクセスし又はこれを受領すること。ただし、コンピュータ・システムを通じて当該データを自国に開示する正当な権限を有する者の合法的なかつ任意の同意が得られる場合に限る。」と規定していることから、Google の同意がなければ越境アクセスはできないと、一般的に解釈されています。

- 日本において、警察が、メールサービス業者に対して当該業者が海外に設置してあるサーバーに保存されたデータの提出を命じたと仮定します（すなわち、違法の疑いが強いデータの提出命令）。当該業者の法務担当者として、違法であることを理由に提出を拒みますか？マイクロソフト社のように令状の取消しを求める法的手続きをとりますか？あるいは、当局の命令に応じて提出に応じますか？

【※ディスカッションは省略】

＜発表者所感＞

- 今回の事案の背景・周辺の事項について調べることで、欧米・米国の個人データ・プライバシーの保護の歴史的経緯、昨今のセーフハーバーやプライバシーシールド、その他国際間の越境データ移転の議論を整理することができた。
- 今回の事案は欧米に関するものであったものの、個人データの越境移転は日本も無縁ではないため、今回の発表を機に、個人データ・プライバシー保護の動向について今後も注視していきたい。
- また、同じゲームに対する個人情報の提供を問う場合であってもゼミ生によって抵抗感の有無、有る場合の感じ方がそれぞれであったことが印象に残った。

以上