2012年3月8日総務省スマホWG

資料3

スマートフォンをめぐる国際的動向

筑波大学　図書館情報メディア系
准教授　石井 夏生利

アメリカの問題意識

- ネットワーク技術のもたらす社会的・経済的利益を維持するためには、信頼が不可欠である。

⇩

- モバイルアプリの急速な普及に対して、プライバシーポリシー策定や実施が停滞している。

⇩

- 透明性の確保が必要

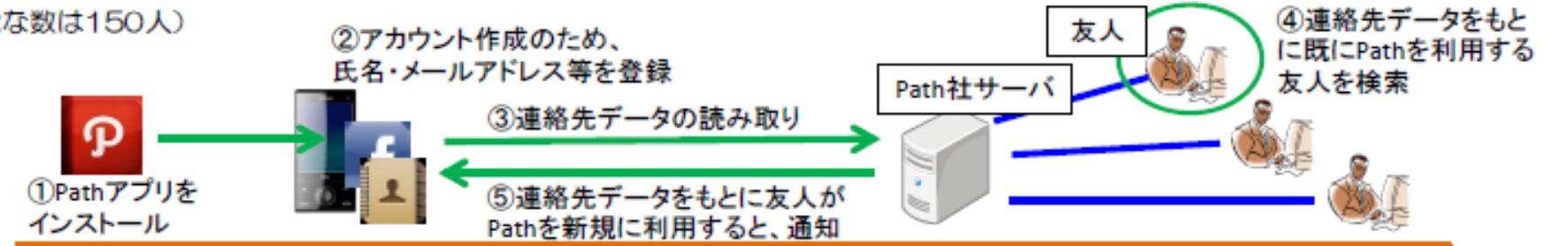
⇩

- 透明性は、消費者の信頼を得るため

Path（iPhoneアプリケーション）概要

Path概要

- 利用者が撮影した画像等を投稿し、当該画像等を友人と共有できる。
- 友人を登録する手段として、検索、招待メールの送信やPathアプリによるFacebook及び端末電話帳情報の読み取りがある。（登録可能な数は150人）



問題点：連絡先をPath社サーバに送信するにあたって、利用者の同意を得られていない可能性

経緯

- 2月7日、「利用者が所持する連絡先をPathアプリがPath社に送信している」旨、個人から指摘。※1
- 2月8日、Path社はこれまで収集した連絡先情報については全て削除したと発表。同日のPathアプリアップデートによりオプトイン機能を備え、また、メールによるオプトアウトも受け付ける旨案内。
- 米国下院エネルギー商業委員会議長Henry A. Waxman議員及び商業製造貿易小委員会議長G.K. Butterfield議員はApple社CEO宛て「AppleのiOSアプリケーション開発者に対するポリシーは、『iPhone』ユーザーとその連絡先の情報に対する保護という点において不十分なのではないかという疑問が生じる」等と記した書簡（2月15日公開）を送付。

Apple社の対応

- 2月15日、Apple社広報担当は、ユーザーの連絡先データを許可なく収集する「iOS」アプリケーション※2は同社ガイドラインに違反しており、今後提供するソフトウェア修正によって連絡先データへのアクセスを希望するアプリケーションは、GPS位置情報と同様に、個別に明確なユーザーの承認を必要とする方向の見直しを検討する予定であると述べた。

※1：Path社CEO Dave Morin氏は「ユーザーがPath上で迅速に友人等を見つけることを支援し、また、友達等のPathへの参加をユーザーに通知するため」と説明した。

カリフォルニア州司法長官との合意

- 2012年2月22日
- プラットフォーム6社(Amazon, Apple, Google, Hewlett-Packard, Microsoft, Research in Motion) とカリフォルニア司法長官が合意。
- 法的拘束力はない。

⇩

- 明示的なプライバシーポリシーの掲示(州オンラインプライバシー保護法)
- プライバシーポリシーを説明するためのデータ領域
- 利用者による違反通報のための手段
- アプリ事業者による対応手続
- 最良の実務の展開

※その他、プラットフォーム事業者による開発者への教育

⇩

- 開発者のプライバシーポリシー違反は、州の不正競争行為又は虚偽広告法に抵触

消費者プライバシー権利章典

- 2012年2月23日付オバマ大統領署名
- 「ネットワーク社会における消費者データプライバシー：グローバル化したデジタル経済において、プライバシーを保護しイノベーションを促進するための枠組み」

4つの要素：消費者プライバシー権利章典、執行可能な実施規範(Codes of Conduct)の策定、効果的な執行、国際的相互運用性

個人データの営利的利用に適用

- 個人のコントロール
- 透明性
- 状況の尊重
- 安全性
- アクセス
- 制限的収集
- 説明責任

Fair Information Practice Principles より発展

消費者プライバシー権利章典の7原則

原則1　個人のコントロール

- 消費者は、企業が消費者からいかなる個人データを収集し、どのように利用するかについて、コントロールを行使する権利を有する。
- 企業は、消費者が意味のある選択を可能にするために、容易に利用でき、アクセス可能な仕組みを提供しなければならない。
- 同様に、同意を撤回し又は制限するための手段を提供しなければならない。

原則2　透明性

- 消費者は、プライバシー及びセキュリティの実務について、容易に理解できアクセス可能な情報を得る権利を有する。
- 消費者が意味ある形でプライバシーリスクを理解し、個人のコントロールを行使するために最も役立つ時期と場所における明示的な情報提供。

消費者プライバシー権利章典の7原則

原則3　状況の尊重

- 消費者は、企業において個人データを収集し、利用し、そして提供する際には、消費者がデータを提供する状況に適合した方法によることを期待する権利を有する。
- 個人データの利用及び開示は、企業と消費者との関係及び消費者が最初にデータを開示した状況と矛盾しない目的に限定すべき。他の目的で利用又は開示する場合には、透明性及び個人のコントロールのための高度な措置が必要。
- 状況に関する重要な要素は、消費者の年齢及び技術への精通度である。子供及び10代の者から取得した個人データに対しては、より高い保護を与えるべき。

原則4　安全性

- 消費者は、安全かつ責任を持って個人データが取り扱われる権利を有する。
- プライバシー及び安全性のリスク評価、責任ある安全保護措置。

消費者プライバシー権利章典の7原則

原則5　アクセス及び正確性

- 消費者は、データの機微性及びデータが不正確な場合に消費者に不利な結果をもたらすリスクに適した態様において、利用可能な書式によって、個人データにアクセスし、訂正する権利を有する。
- 企業は適切な措置を講じること。
- 表現の自由及び報道の自由に適合した解釈を行うこと。
- 措置を講じる際の考慮事項：企業が収集又は維持する個人データに関する規模、範囲及び機微性、及び、その利用が消費者に経済的、物理的又は具体的被害を被らせる可能性。

原則6　制限的収集

- 消費者は、個人データを収集及び保有する企業に適切な制限を課す権利を有する。
- 個人データの収集を目的達成に必要な範囲に限定。
- 不要になったデータの破棄又は匿名化。

消費者プライバシー権利章典の7原則

原則7　説明責任

- 消費者は、企業が個人データを取り扱う際に、プライバシー権利章典を確実に厳守するための適切な措置とともに行わせる権利を有する。
- 執行機関及び消費者への説明。
- 従業員の訓練と評価、監査の実施。
- 個人データを受領する第三者に対する契約上の義務づけ。

個人のコントロールと「追跡拒否」(Do not track)

- 個人のコントロールに関する原則が有する2つの側面

- 個人データ収集時における選択の提供

- 選択に対する消費者の責任

- Do Not Trackの仕組みは、第三者による個人データの取扱いに対する一定のコントロールを可能にする。

消費者保護の分野における自己情報コントロール

Do Not Track

- 2010年12月　FTCスタッフ中間報告「急変する時代の消費者プライバシー保護」

⇩

- 統一的かつ包括的な消費者選択の仕組み

⇩

- クッキーに似た設定をブラウザに追加

⇩

- HTTPリクエストに「DNT:1」を追加し、信号を送信

Digital Advertising Allianceによる追跡拒否機能のサポート(9ヶ月以内に実装)

2012年2月2月23日付ウォールストリートジャーナルの記事(Web Firms to Adopt 'No Track Button')(http://online.wsj.com/article/SB10001424052970203960804577239774264364692.html)より

消費者プライバシー権利章典の「個人データ」

- 営利事業者が取り扱う消費者に関する多様なデータをカバーするための柔軟化

⇩

- 集積されたデータを含むあらゆるデータであって、特定個人と結びつく(linkable)もの
- 特定のコンピュータ又は他の装置と連結されるデータを含む。例えば、スマートフォンの識別子、使用履歴(usage profile)を築き上げる家庭用コンピュータなど

identifiableでなくてもよい

EUの個人データ概念の変更

- 1995年EU個人データ保護指令

  「識別された、又は、識別されうる自然人(データ主体)に関するすべての情報をいう;識別されうる自然人とは、とりわけ、個人識別番号、又は、その人の肉体的、生理的、精神的、経済的、文化的、若しくは社会的アイデンティティーに特有な1つ以上の要素を参照することよって、直接又は間接に識別することができる者をいう」(第2条(a)号)

⇩ 識別性の排除

- EUデータ保護規則提案

  「個人データは、データ主体に関連する(relating to)あらゆる情報を意味する」(第4条(2)項) 氏名、写真、電子メールアドレス、口座情報、ソーシャル・ネットワーキングサイトへの投稿、医療情報又はコンピュータのIPアドレスが含まれる。

消費者データプライバシー立法

- 消費者プライバシー権利章典の成文化
- FTCによる直接的法執行
- 執行可能なセーフハーバーを通じた法的確実性
  - 消費者プライバシー権利章典に対応する実務規範を審査するFTCの排他的権限
  - FTCが審査・承認した実務規範を遵守する企業に対する法執行の自制
- 消費者データプライバシー保護における連邦と州の役割の均衡
- 既存の連邦データプライバシー法における効果的な保護の維持

1　二重の負担を伴わない包括的なプライバシー保護の設定

2　矛盾又は混乱をもたらす義務規定の改正

- セキュリティ侵害通知のための全国的基準の策定
  - 特定種類の個人データに関して、無権限アクセスが生じた場合に消費者への通知を義務づける連邦法の制定(センシティブデータを想定)。

消費者プライバシー権利章典の考え方

- 消費者プライバシーの分野における「個人データ」(個人情報)概念の拡大：identifiableからlinkableへ

→適用範囲は広く

- 他国との相互運用性：実務規範をプライバシー保護の相互認証に関する基本に据える(APECの越境プライバシールール、EUデータ保護指令)。

→自主的取組をベースに

- FTCによる直接的執行

→サンクションを担保

意味ある選択を確保するための情報提供・透明性

※後述する「子供のためのモバイルアプリ」の考え方も共通的

(参考)

APECの取組：CBPR（Cross Border Privacy Rules）

- 組織が他のAPEC参加エコノミーへの越境移転を行うための体制が検討されている。

エコノミーによるCBPRへの参加条件

- CPEAに参加していること
- CBPRへの参加表明書の提出
- APECの承認した責任団体(Accountability Agent)の1つを少なくとも利用すること。

※責任団体とは、CBPRの認証を求める企業によるプライバシー・ポリシー及び実務が、体制の基準となる要求事項を満たしている旨を証明する団体であって、APECの承認を受けたものをいう。

(参考)

CBPRの4つの要素

- 自己評価(self-assessment)　組織は、プライバシーポリシー及び実務がAPECのプライバシー・フレームワークの要求事項を満たしていること。
- 適合性審査(compliance review)　責任団体になるための認定基準の充足、責任団体による適合性審査。
- 認証・受入れ(recognition/acceptance)
  責任団体がCBPRシステムに準拠した旨を認証した組織一覧の公表。
- 紛争解決及び執行(dispute resolution and enforcement)
  責任団体及びプライバシー執行機関による執行

違反組織への是正要求、CBPR参加組織からの除名、責任団体の認証シールの一時利用停止、違反組織の公表、プライバシー執行機関等への照会、その他金銭的制裁等

(参考)

1995年EUデータ保護指令改正提案の公表

- 2012年1月25日
- オンライン・プライバシー権の強化
- 欧州のデジタル経済の促進

目的

- 技術の発展とグローバル化により、データの取扱いに関する態様が大きく変化した。
- 27の加盟国が制定した法律はそれぞれに異なっており、執行の際に不一致をもたらしている。
- 単一の法を設ければ、加盟国の分散状態を解消し、事業者に課せられている割高な管理費用を軽減することができる(年間約23億ユーロの負担軽減が想定)。

背景

その他、一般的な通知義務を廃止することで、年間約1億3000万ユーロの削減が期待されている。

(参考)

提出された提案

- 個人データの取扱いに係る個人の保護と当該データの自由な移動に関する欧州議会及び理事会の規則(一般データ保護規則)提案
- 所管の機関による刑事犯罪の予防、捜査、探知若しくは起訴又は刑事罰の執行のための個人データの取扱いにかかる個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令提案

(参考)

主な改正点

- 「指令」から「規則」へ
- 「同意」は「明示的同意」
- データ保護原則の変更
- 忘れてもらう権利
- データ・ポータビリティの権利
- データ保護・バイ・デザイン
- 個人データ侵害の通知/連絡制度
- データ保護影響評価
- 「十分な保護レベル」と独立監視機関
- 拘束的企業ルール
- データ保護に関する認証の仕組み
- 第29条作業部会から欧州データ保護委員会への改組
- 全世界の総売上2%を上限とする罰金措置

(参考)

EUの域外適用(第3条)

- 本規則は、EU内で設立された管理者又は取扱者の事業活動に関する個人データの取扱いに適用。
- 本規則は、次に掲げる場合、EU内で設立されていない管理者において、EU内に居住するデータ主体の個人データを取り扱う場合に適用。

  (a) EU内の当該データ主体に対する商品又はサービスの提供

  (b) 彼らの行動を監視
- EU内では設立されていないが、加盟国の国内法が国際法に基づいて適用される場所では、管理者による個人データの取扱いに本規則が適用。

(参考)

忘れてもらう権利(The right to be forgotten)

- 1995年EUデータ保護指令第12条(b)号

「加盟国は、全てのデータ主体に対し、管理者から次に定めるものを取得する権利を保障しなければならない。

(b)　適切な場合には、特にデータの不完全又は不正確な性質のために、この指令の規定に従わないで取り扱われたデータの修正、消去又はブロック」

⇩

新規則案では「ブロック」は使われず。

- 精緻化し、具体化したのが「忘れてもらう権利」

(参考)

「忘れてもらう権利」の原則論(第17条1項)

- 管理者に対し、個人データを削除させる権利
- 管理者に対し、個人データの拡散を停止させる権利

⇧

- データの収集又は取扱目的との関連で、必要でなくなった場合
- データ主体が同意を撤回した場合、同意を与えた保存期間を徒過した場合、データを取り扱うための他の法的根拠がない場合
- データ主体が個人データの取扱いに異議を申し立てた場合
- データの取扱いが他の理由により本規則に違反する場合

(参考)

あらゆるデータの削除(第17条2項)

- データ管理者が個人データを公開していた場合は、当該データを取り扱っている第三者に対し、データ主体がその個人データに関するすべてのリンク、コピー又は複製の削除を要請している旨を通知するための措置を講じなければならない。
- 管理者において、第三者による個人データの公開を許可していた場合、管理者は、当該公開に責任を負う。

(参考)

忘れてもらう権利の例外（第17条3項）

- 表現の自由の権利を行使するため
- 公衆衛生分野における公の利益がある場合
- 歴史的、統計的及び科学的な研究を行うため
- 個人データを保有する法的義務を遵守するため
- 本規則に基づき個人データの取扱いが制限される場合

子供のためのモバイルアプリ

- 2012年2月16日付FTCスタッフレポート
- 「子供のためのモバイルアプリ：現行のプライバシー開示への失望」

⇩

- アプリの数は急速に増加しているが、プライバシー実務に関する情報提供が欠如

⇩

- 「本報告書は、親が子供のためにモバイルアプリをダウンロードするに先だって入手できる情報が欠如していることを強調するとともに、業界に対し、自らのデータ実務に関する透明性を拡大して提供すことを求める。」
- “informed decisions”の重要性

自己情報(親による子供の情報)のコントロール

アプリの調査①

- 2011年7月、Apple App Storeの8000アプリとAndroid Marketの3600アプリを調査(うち、“kids”というカテゴリに属する各200のアプリが主たる調査対象)。
- ほとんどのアプリが$0.99以下で提供。
- アンドロイドはアプリに同意画面を要求しているが、アプリが同意を得る理由、当該アクセスによるアプリの活動、アプリが第三者と情報を共有するか否かが明確に説明されていない。
- 子供用に作られた182のアンドロイドアプリのうち、約24%は、モバイル機器から送出される情報等へのアクセスなくしてアプリを使うことができる(特段の同意は求められていない)が、約76%は少なくとも1つの同意を求めている。同意を求めるアプリのうち、約60%は「全てのインターネットアクセス」への「同意」を求めている。
- アップルアプリを提供する際には審査が行われるが、審査手順の詳細は明らかでない。

アプリの調査②

- 位置情報は、位置情報サービスのon/off機能が提供されるほか、アイコンの表示により警告を出す仕組みが用いられている。
- いずれのアプリについても、開発者のプライバシーポリシーがアプリの実務を司っている。
- アンドロイドアプリでは、200のアプリのうち3つ(1.5%)のみが「同意」を目的とした情報提供を行っていた。それでもなお、収集される情報、収集する者、利用方法、他者と共有されるか否かについての情報は特定されていない。
- アップルのアプリ宣伝ページでは、情報の収集利用についての情報を提供するものはほとんど見られなかった。
- 400のキッズアプリ宣伝ページのうち、13%は開発者のプライバシーポリシーへとつながるリンクが付されていた。
- 400のアプリ宣伝ページのうち、2ページ(0.5%)のみが、データ収集及び共有に関する情報を提供する開発者の待受けページにリンクした。

児童オンラインプライバシー保護法

- Children's Online Privacy Protection Act of 1998, COPPA
- Children's Online Protection Rule
- 商用ウェブサイト又はオンライン・サービスの管理者において、インターネットを通じて、13歳未満の児童に関する個人情報を収集する場合に、親に対する事前通知、及び、親からの事前の同意取得が義務づけられている。

⇩

Children's Online Privacy Protection Ruleの改正

- 定義：「個人情報」に、クッキーが保有する情報、機器番号、IPアドレス、位置情報、写真、ビデオ、音声ファイルなどを含める(消費者のインターネット活動を追跡するための情報を含める)。その他「収集」に関する改正。
- 親への通知：適時に簡潔な通知の提供
- 親の同意の仕組み：同意の立証を裏付けるための新たな仕組みの導入
- 秘密性と安全性の義務強化
- セーフ・ハーバー：FTCの監督強化

勧告事項

- アプリストア、開発者及びアプリ内でサービスを提供する第三者は、親に対する積極的な情報提供を行うべきである。
- アプリ開発者は、データ実務に関する情報を単純かつ簡潔な開示態様で提供すべきである。
- 開発者は、アプリがソーシャルメディアに接続される場合、又は、アプリを通じてターゲティング広告を受け入れる場合に警告を発するべきである。
- アプリを通じて情報を収集する第三者は、容易にアクセスできる方法により自らのプライバシー実務を開示すべきである。
- アプリストアは、アプリ市場のゲートキーパーとして、情報開示のための指定領域の提供、警告を発するための標準アイコンの提供等に加え、開発者に情報開示を強制するための一層の取組を行うべきである。

オンラインにおける児童の保護に関するOECD理事会勧告

- 2012年2月16日採択
- オンライン上の児童を保護するための政策を形成するに際して、政府及び他の全ての利害関係者が考慮すべき諸原則
  - 権限の付与：全ての利害関係者の責任負担、リスクの評価及び最小化等のための児童及び親への権限付与
  - 均衡性及び基本的価値：保護のための政策とリスクの均衡性、効率性及び公平性
  - 柔軟性：年齢、発達段階及び要保護性に適した保護策
- オンライン上の児童を保護するための国内レベルでの政策を形成するに際して、政府が実施すべき事項
- 国際レベルにおいて政府が実施すべき事項