Vol.2016-DPS-168 No.5
Vol.2016-SPT-21 No.5
Vol.2016-EIP-74 No.5
2016/11/17

ネットワーク接続機器の位置情報に関するプライバシー・個人情報保護制度の動向

小向太郎[†1]

コンピュータ処理能力の向上と，データ収集可能な情報の増大を背景に，大量のデータが分析・利用されるようになっている．特に，スマートフォンに代表されるネットワーク接続機器には，位置情報を取得する機能が登載されていることが多く，さまざまな分野で利用が期待されている．しかし，位置情報は，人の行動と密接に結びついている場合も多く，プライバシーや個人情報保護の観点からの問題も懸念されている．本稿では，こうした位置情報に関する各国の制度を比較し，位置情報に関するプライバシー・個人情報保護制度のあり方について検討する．

A Comparative Legal Study on Location Data Privacy

TARO KOMUKAI[†1]

This paper focuses on privacy and data protection associated with location data collected from networked devices. While use of location data could bring us variety of convenient services, it also could be a curse to serious privacy concern because location data could be collected, used or disclosed while data subject does not recognize it. The aim of this paper is to compare the relevant discussions in the EU, the U.S. and Japan, and reach a suggestion for appropriate solution.

1.ビッグデータと位置情報

1.1 位置情報への期待

コンピュータ処理能力の向上と，データ収集可能な情報の増大を背景に，大量のデータが分析・利用されるようになっている．特に，スマートフォンに代表されるネットワーク接続機器には，位置情報を取得する機能が登載されていることが多く,さまざまな分野で利用が期待されている．例えば，情報通信審議会は,「IoT/ビッグデータ時代に向けた新たな情報通信政策の在り方」についての諮問に対して 2015 年 9 月に第二次中間答申を公表している．このなかでは，重点取組分野の一つとして「通信」をあげ,「革新的なサービスの創出に向けたデータ利活用が検討されている中で，特に，個人に応じたきめ細かいサービスの実現に不可欠となる，性別や年齢，位置情報といった個人の属性や行動履歴，生活環境に関するデータが注目されて[1]」いるとしている．

しかし，位置情報は，人の行動と密接に結びついている場合も多く，これらの情報が本人の望まない使われ方をされるとプライバシーや個人情報保護上の問題を生じることが懸念されている．情報通信審議会答申の中でも,「個人情報保護法や関係のガイドラインにおいては，位置情報等の利活用についてルールが明確化されておらず，関連事業者による取組を一層進めるため，具体的なユースケースを踏まえた取扱いの ルールの整備が不可欠となっている[1]」と言う指摘がされている．

本稿では，ネットワークに接続する機器が取得する位置情報について，我が国における法的位置付けや，欧米における保護の動向を比較し,位置情報に関するプライバシー・個人情報保護制度のあり方について検討する．

1.2 利用分野

最近注目を集めている IoT（Internet of Things）やビッグデータ技術において利用されるデータのなかでも，特に位置情報を含む情報は，社会全体の利益や利用者の利便性に寄与するソリューションを実現しうるものとして，期待を集めている．具体的な利用分野も幅広く，例えば下記のようなソリューションの実現のためには，位置に関する情報をネットワーク経由で把握することが前提となることが多い．

- 都市計画への利用（交通システムや防災対策の最適化）
- 情報提供（公共交通機関の混雑状況や渋滞情報の提供）
- ターゲッティング広告（所在エリアに応じた広告や割引クーポンの提供）
- レコメンデーションやサービスのカスタマイズ（サービスのきめ細かな調整）

†1 日本大学
Nihon University

Vol.2016-DPS-168 No.5
Vol.2016-SPT-21 No.5
Vol.2016-EIP-74 No.5
2016/11/17

- 行動支援型サービスの提供（経路情報や地域案内，障害者等への移動支援等）
- 犯罪捜査や治安維持への利用（犯罪やテロの予防，犯罪捜査）

1.3 位置情報の収集技術

ネットワーク接続機器等によって収集される位置情報としては，表１のようなものが考えられる．

（表 1）位置情報収集技術の例

端末等種別	ネットワーク接続機器（例）	収集情報（例）
インターネット端末	PC，スマートフォン，タブレット端末，ゲーム機	GPS 位置情報，基地局情報，Wifi アクセスポイント
自動車，重機	カーナビゲーション・システム，自動運転や電気自動車の制御装置，遠隔操作システム	GPS 位置情報，走行情報
カメラ	監視カメラ，デジタルカメラ	顔認識等によるトレース情報，GPS による撮影地情報
ID カード等	POS レジ，IC カードリーダ，RFID リーダ，自動改札	購買場所と登録住所，交通機関の利用経路

さまざまな機器がネットワークで接続されるようになり，情報が大量に収集処理されることで，従来はあまり意識されなかった POS レジや IC カードリーダによって収集される情報も，位置情報としての意味を持つようになってきている．こうした情報の取扱についても，今後は注意が必要になってくるであろう．

2. わが国における法的位置づけ

2.1 個人情報保護法上の義務

位置情報は単独では個人情報に該当しない場合もあるが，「生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの」が含まれている場合や，そうした情報と「容易に照合することができ，それにより特定の個人を識別することができることとなる」場合には，個人情報となる（個人情報保護法 2 条 1 項）．個人情報取扱事業者は取扱う個人情報について，利用できる目的をできる限り特定し（15 条），公表等することと（18 条）その目的の範囲で利用すること（16 条）が求められる．

現行法上は，利用目的を特定・公表して，その範囲で利用するのであれば，本人の同意等は求められていない．ただし，情報の性格によってはできるだけ本人の意思を反映させるべきではないかという意見はあり，例えば総務省「パーソナルデータの利用・流通に関する研究会報告書」では，パーソナルデータのなかでも慎重な取扱いが求められるものについては取扱に際して同意を得るべきであるとしている．そして，そうした情報の例として「継続的に収集される購買・貸出履歴，視聴履歴，位置情報等」があげられている（総務省「パーソナルデータの利用・流通に関する研究会報告書~パーソナルデータの適正な利用・流通の促進に向けた方策~」（2013 年 6 月）28-30 頁）．なお，個人情報保護法は，個人データ（電子化または体系化された個人情報）の第三者提供には原則として本人の同意が必要であるとしており（23 条），本人の同意がなくても第三者に提供できるのは，法令に基づく場合や緊急性等がある場合（23 条 1 項）のほかに，オプトアウト（23 条 2 項），委託先への提供（23 条 4 項 1 号），事業承継（23 条 4 項 2 号），共同利用（23 条 4 項 3 号）のいずれかに該当する場合に限られる．

2.2 携帯電話事業者と通信の秘密

携帯電話事業者が取扱う位置情報については，通信の秘密との関係が問題となる[2]．携帯電話事業者が取得する位置情報には，「個別の通信を行った基地局の位置情報」「位置登録情報（端末所在地を基地局単位等で把握する情報）」「GPS 位置情報（GPS 機能により取得する情報）」の 3 種類がある．このうち「個別の通信を行った基地局の位置情報」は，通信の秘密であるとされる．通信の秘密として保護される情報としては，通信内容以外に，個別の通信の通信当事者がどこの誰であるかということや，いつ通信を行ったかということも含まれると考えられており，「個別の通信を行った基地局の位置情報」は，こういった情報に該当する．そして，通信の秘密に当たる情報の取得は，電気通信サービスの提供に必要な範囲で利用できるほかは，正当防衛や緊急避難などの違法性阻却事由が認められる場合にのみ許される [3]．さらに，総務省のガイドラインでは「位置登録情報」「GPS 位置情報」についても，「ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が 高い上に，通信とも密接に関係する事項であるから，通信の秘密に準じて強く保護することが適当である[4]」と位置づけ，情報の取得に際して利用者の同意を取得すること等を求めている．

なお，GPS 情報は，電気通信事業者以外にも，いわゆるスマホアプリ等の提供者によって利用されることがある．当初から，一部のアプリでは利用者の情報を同意なく送信していることや，情報を取得・利用する旨の同意をとっている場合でも，どのような情報を何に利用するのかは詳しく表示されていないまま，利用者は反射的に同意ボタンを

Vol.2016-DPS-168 No.5
Vol.2016-SPT-21 No.5
Vol.2016-EIP-74 No.5
2016/11/17

押してしまっていることが，問題だと指摘されていた．

この問題については，総務省が 2012 年 8 月に，「スマートフォン プライバシー イニシアティブ」を公表し，アプリが利用者情報を外部送信したり蓄積したりしている場合には，どのような情報が取得・利用されているかを分かりやすく記述したプライバシー･ポリシーを公表することや、電話帳・位置情報・通信履歴等のプライバシー性の高い情報を取得する際の利用者の同意を取得することを推奨している[5]．ただし，このような取り組みを法的に求めるものではなく，事業者の自主規制を促すものとなっている．

2.3 Wi-Fi アクセスと位置情報

携帯電話事業者に限らず，公衆無線 LAN（Wi-Fi）へのアクセスを提供している事業者は，利用者がどのアクセスポイントを利用したかという情報を取得しうる．Wi-Fi の設置者は，各アクセスポイントが設置されている場所を通常把握しているので，端末利用者がアクセスポイントにどのアクセスポイントにアクセスしたかが分かれば，利用者がそのアクセスポイントのカバーエリアにいた事がわかる．これも端末利用者の位置情報であるといえる．

こうした情報については，携帯電話事業者の基地局情報と同様に，端末利用者が通信を行っている場合のアクセスポイントは通信の秘密，端末利用者がアクセスポイントにアクセスしているだけの場合に取得される情報はその他の位置情報であると考えられている[6]．

3. 欧米の動向

3.1 欧州の動向

EU では，1995 年に採択された「個人データ処理に係る個人の保護および当該データの自由な移動に関する欧州議会および理事会の指令（EU 個人データ保護指令）」に基づいて個人情報保護に関する制度が各構成国で整備されている．2012 年 1 月には，EU 域内の個人情報保護をさらに確保するために,「個人データの取扱いに係る個人の保護および当該データの自由な移動に関する欧州議会および理事会の規則案（GDPR）」が提案され，2016 年 5 月に発効し，2018 年 5 月に施行される予定である．構成国に立法を求める「指令」から，直接適用される「規則」に変更されるとともに，環境の変化に対応するための数多くの保護規定が追加されている．

EU 個人データ保護指令では,個人データ（personal data）の処理に本人の同意を求めることが基本的な枠組みとして採用されていたが，GDPR では，有効な同意とみなされるための要件が明確化されるなど，さらに本人によるコントロールが重視されている．

GDPR が保護の対象とする個人データは，「識別（identify）された，または識別可能な自然人に関するあらゆる情報」と定義されている．ここでいう識別可能な自然人とは「直接的であるか間接的であるかを問わず特に識別子を参照することで，識別されるもの」をいう．そして，識別子には「名前，識別番号，位置情報，オンライン識別子や，その人物の物理的，生理的，遺伝子的，精神的，経済的，文化的または社会的な固有性として，単独または複数組み合わせによって特定される要素」が該当する（第 4 条（1））．したがって，位置情報を含む情報は，個人データとして GDPR の保護を受ける．

また，2002 年に採択され，2006 年および 2009 年に改正されている「個人データの保護および電子通信分野のプライバシー保護に関する欧州議会および理事会の指令（電子通信プライバシー指令）」には，位置情報に関する特別の規定がある．位置情報は「電気通信網または電子通信サービスにおいて処理される情報であり，公衆電気通信サービスのユーザ端末機器の地理的な位置を示す情報」と定義され，その処理については次のように定められている[7]．

第 9 条　位置情報a

1. 公衆電気通信ネットワークまたは広く利用可能な電子通信サービスの利用者・加入者に関する位置情報は，匿名化されている場合か，（通信サービス以外の）付加価値サービスの提供のために必要な範囲及び期間に関して，利用者が同意をしている場合に限って，処理することができる．サービス提供者は，位置情報の種類，利用目的，処理期間、データの第三者の有無について，同意取得に先立って，利用者・加入者に知らせなければならない．利用者・加入者は，位置情報の処理に関する同意を，いつでも撤回することができる．
2. 位置情報について利用者・加入者の同意が得られている場合には、利用者・加入者に対して，シンプルな手段によって無料で，当該ネットワークへの接続や電子通信の伝送が行われるたびに，これらの情報の処理をいつでも拒否することを常に可能にしておかなければならない。
3. 本条 1 項および 2 項に基づく位置情報の処理は，公衆電気通信ネットワークまたは広く利用可能な電子通信サービスの提供者によって権限を付与された者によって行われる場合か，（通信サービス以外の）付加価値サービスの提供者によって権限を付与された者によって行われる場合であって当該付加価値サービスの提供目的に必要なものに限られている場合に，限定されなければならない。

a トラフィック・データについては別の規定（6 条）があるため，本条の「位置情報」は全て「トラフィック・データ以外の位置情報」と規定されているが，本稿の訳では単に「位置情報」としている．

Vol.2016-DPS-168 No.5
Vol.2016-SPT-21 No.5
Vol.2016-EIP-74 No.5
2016/11/17

電子通信プライバシー指令は，GDPR の成立をうけて改正が検討されており，データ保護指令第 29 条に基づいて設置され他諮問機関である 29 条作業部会が，改正のあり方について意見書を公表している[8]. この意見書なかで 29 条作業部会は，現行の位置情報に関する規定が通信事業者や通信サービスのプロバイダに限られており，例えばアプリケーション開発事業者が対象になっていないことなどを指摘し，規定の整理に合わせて対象を拡大することが望ましいとして，次のような考えを示している.

「現行の電子通信プライバシー指令におけるトラフィック・データと位置情報に関する規定を統合することによって，改定後の電子プライバシーに関する規定は，全ての関係者に向けた規定であることが明確になりうる．これらのメタデータの処理に対して同意を要求することによって，改正電子プライバシー規定は，GDPR の第 6 条が定めるデータ主体の同意と同等の強い法的基準に基づくハイレベルな保護を提供することになる．通信の秘密は，民主主義社会の核心的な権利である．したがって，通信およびそれに関連するメタデータには，より厳格なルールが求められる．特に，現代の通信技術は，表には現れない方法や少なくとも人々が完全には気づかない方法で，度を超えた大量のデータの収集を可能にしているからである．通信を提供するという特別な利用目的を超えて，これらのデータを収集，処理，および利用を行うことは，利用者が適切な情報提供を受けたうえで同意をした場合にのみ許される．以上のような理由から，本作業部会は欧州委員会に対して，電子通信のより良いセキュリティ保護のために，トラフィック・データと位置情報のようなメタデータの処理に対して調和の取れた同意取得を義務付けることを勧告する．この同意取得義務は，全てのトラフィック・データと位置情報について適用されるべきであり，ユーザ端末のセンサーによって生成される場合も含むとすべきである．この新たなルールは，これらのデータを収集・処理する全ての者に対して適用されなければならない（14 頁）」

3.2 米国の動向

米国で消費者プライバシーを所轄する連邦取引委員会（FTC: Federal Trade Commission）は，2012 年 3 月に「急変する時代の消費者プライバシー保護」という報告書を取りまとめている[9]. FTC は，この報告書が示すフレームワークの対象を「特定の消費者，コンピュータその他のデバイスに合理的に結びつけうる消費者に関する情報を収集または利用する営利主体であり，収集する消費者情報が 5,000 件未満で機微でない情報に限られ他に提供を行っていないものを除く（22 頁）」としている．また，このフレームワークでは，本人意思の反映を重視しており，プライバシー・バイ・デザイン，シンプルで分かりやすい消費者の選択，透明性を重要な要素としてあげている．さらに，消費者が自分のデータに関する決定を行うような状況では選択の機会が与えられるべきであり，（1）データが収集される際に示された方法と大きく異なる方法で利用される場合と（2）ある目的のためにセンシティブ情報を収集する場合には，積極的な同意の表明を得るべきである」としている. そして,「子供に関するデータ, 金融情報と健康情報, 社会保障番号，および一定の位置情報は，少なくともセンシティブ・データ」として扱うという考えが示されている（47 頁，注 214）．ただし，これらは事業者に対するベストプライティスを示したものと位置づけられ，執行の指針を直接示したものではない.

一方で，FTC は法執行についても多くの実績がある．FTC 法 5 条の「商業活動に関わる不公正な競争手段と，商業活動に関わる不公正または欺瞞的な行為または慣行は，違法であることがここに宣言される（15 U.S.C. § 45(a)(1).）」と規定している．この規定が FTC による法執行の根拠となっており，自社のプライバシー・ポリシーや利用規約で個人情報の利用を拒否できるかのように記述しているにもかかわらず，対応を十分にしていなかったことなどが，欺瞞的とされているケースが多い[10].

また, 電気通信事業者に対する規制を所轄する FCC は，2012 年に，「ロケーション・ベースド・サービス」という報告書公表している[11]. この報告書は, 位置情報を利用したサービスの重要性と今後の可能性について検討を行っており，特にプライバシーに対する懸念がこの分野での最重要課題の 1 つであるという認識を示している．そして，ロケーションテストサービスを提供する事業者に，①製品の開発段階開発初期段階でのうらやましいでも入るプライバシーの配慮．②データのセキュリティ，③通知の時期と内容の充実，④データの最小化，といった取り組みを求めている．そして，政府と産業が合意して位置情報利用ビジネスとプライバシーの問題とのバランスを最適化していくべきだとする一方で，FCC としてはあわせて監視も続け，さらに次のステップが必要かどうかについても検討する可能性があることを表明している（40-41 頁）.

さらに FCC は，ブロードバンドサービスを始めとする電気通信サービスに関する消費者プライバシーの保護に関して，2016 年 4 月に規則制定案告示（NPRM: Notice of Proposed Rulemaking）を公表し，規則制定の手続きに入っている[12].

FCC の規則制定手続きでは多くの場合, まず規則制定案告示が公表される. このかなで事案に関する説明と FCC の考え方が示され，これに対する関係者の意見が広く求められる．提出された意見を勘案して、規則がまとめられることになる[13].

今回の規則制定提案では，特に配慮が必要な情報の候補

Vol.2016-DPS-168 No.5
Vol.2016-SPT-21 No.5
Vol.2016-EIP-74 No.5
2016/11/17

について，次のように関係者の意見を求めている．

「特定の種類の情報の保護．例えば，社会保障番号，金融口座情報，地理空間情報などは，すでに顧客識別情報の定義に含まれているが，これら特定のタイプの情報について，特に機微性が高いという理由で特別な扱いをすべきかどうかについても，この規則制定案告示において意見を求めることとしたい（10 頁）」

さらに，特に地理空間情報（Geo-location）については，次のような考えを示したうえで，この解釈に対する関係者意見を求めている．

「委員会としては，顧客または顧客の端末の，物理的または地理的な位置情報に関する情報については，ブロードバンド・インターネット・アクセス・サービス提供事業者が当該情報を取得するために用いる技術や方式がどのようなものであるかに関わらず，ブロードバンドにおける顧客に帰属するネットワーク情報（CPNI: Customer Proprietary Network Information b）とみなすことを提案する．CPNI の法的な定義には，顧客が加入した電気通信サービスの位置に関連する情報が含まれる．委員会は，顧客による電気通信サービスの利用が行われる位置は，明確に CNPI に該当すると考える（16 頁）」

3.3 まとめにかえて

以上のように，EU および米国でも，位置情報に関するプライバシー・個人情報保護に関する検討が現在も行われている．EU では，GDPR の制定を踏まえて，電子通信プライバシー指令の改正が検討されており，位置情報については，より広い範囲の保護をすべきではないかという意見が出されている．米国でも，消費者プライバシー政策を担当する FTC と，電気通信に関する規制を所掌する FCC がともに位置情報に関するプライバシー保護について検討を行っている．

我が国では，携帯電話事業者に関する位置情報に関しては厳格な配慮が求められており，この点では欧米と比較してもより保護されているとも言える．しかし，それ以外の分野に関しては，その他の個人情報と法的保護の内容に変わりがない．

そもそも，わが国の個人情報保護法においては，個人情報の収集前に利用目的を特定・公表して，その範囲で利用するのであれば，利用一般について本人の同意やプライバシーへの配慮を求める規定がない．

今回の法改正では，「要配慮個人情報」に関する規定が設けられ，「本人の人種，信条，社会的身分， 病歴，犯罪の経歴，犯罪により害を被った事実その他本人に対する不当な差別，偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして 政令で定める記述等が含まれる個人情報（第 2 条第 3 項）の取得には，法令に基づく場合等の正当な理由がある場合を除き，本人の同意が求められることになっている．しかし，それ以外の情報については，情報の利用目的が情報主体の意思に反するものであっても，個人情報を収集した事業者の内部利用については，利用自体を止めさせる直接の法的根拠はない．

EU の制度は，本人の同意を原則として，その同意をいつでも撤回できる権利を認めており，本人の意志の反映を保障している． 米国の制度は，消費者保護をベースに，不公正または欺瞞的行為または慣行を禁止するという形をとっており，他国の個人情報保護制度とは体系が異なる．しかし，消費者の期待を裏切る悪質な行為は FTC 法 5 条に基づき執行が可能であり，積極的な法執行と相まって，実質的に事業者に消費者の意思の反映を求めることに実効を挙げていると評価してよいであろう．個人情報の利用目的について，日米欧の制度上の要求事項の概要を比較したものが（表 2）である．

（表 2）本人の意思を反映する規定（概要）

	取得	保存	提供
EU	本人の同意，法定の利用，公共の利益等	同意の撤回の保障	同意の撤回の保障
米国	不公正または欺瞞的な行為または慣行の禁止	不公正または欺瞞的な行為または慣行の禁止	不公正または欺瞞的な行為または慣行の禁止
日本	利用目的の通知. 公表, 適正取得	目的外利用の禁止	本人の同意

IoT やビッグデータ技術によって，位置情報を始めとするさまざまな情報が，当初予想されていなかった利用が発生する懸念が高まっている．こうした懸念を考慮に入れた場合に，本人のコントロールをどのように及ぼすべきかという議論が，各国で進んでいる．特に，本人の同意が，有効な同意であるかどうかということや，どのような射程で同意がなされているかを，新たな状況のもとでどのように考えるべきかが焦点になっている．我が国でもこうした議論が行われてはいるが，わが国の議論は基礎となる法律上の根拠に欠ける面があるのは否めない．

b CPNI: Customer Proprietary Network Information に該当するかどうかは，1996 年通信法 222 条が定める顧客情報のプライバシーに関する規定（47 U.S.C. § 222.）の規制の適用について判断するための基準となっている．

Vol.2016-DPS-168 No.5
Vol.2016-SPT-21 No.5
Vol.2016-EIP-74 No.5
2016/11/17

位置情報のように，本人の意思反映自体が難しいとされている情報の保護について議論を進める場合でも，そもそも本人意思の反映について，さらに法的な保障が必要かどうかについて，まず議論される必要がある．

参考文献

[1] 情報通信審議会「IoT/ビッグデータ時代に向けた新たな情報通信政策の在り方（平成 27 年 9 月 25 日付け諮問第 23 号)」第二次中間答申（2015 年 9 月）24 頁
[2] 小向太郎「ライフログの利活用と法律問題」ジュリスト 1464 号（2014 年 3 月）53-58 頁.
[3] 多賀谷一照他編著『電気通信事業法逐条解説』(財団法人電気通信振興会，2008）37-41 頁参照.
[4] 総務省「電気通信事業における個人情報保護に関するガイドライン（平成 16 年総 務省告示第 695 号。最終改正平成 27 年総務省告示第 216 号）の解説」46-48 頁.
[5] 利用者視点を踏まえた ICT サービスに係る 諸問題に関する研究会「スマートフォン　プライバシー　イニシアティブ」（2012 年 8 月）.
[6] 藤波恒一「位置情報に関するプライバシーの適切な保護と社会的利用の両立」ジュリスト 1484 号（2015 年 9 月）87 頁.
[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[8] Article 29 Data Protection Working Party, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), Adopted on 19 July 2016, WP 240.
[9] FTC, Protecting Consumer Privacy in an Era of Rapid Change (2012).
[10] 小向太郎，「米国 FTC の消費者プライバシーに関する法執行の動向」，堀部政男編『情報通信法制の論点分析』(商事法務，2015)151-162 頁.
[11] FCC Wireless Communications Bureau, Location-Based Services - An overview of opportunities and other considerations, May 2012.
[12] FCC, Notice of Proposed Rulemaking: In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Released: April 1, 2016.
[13] FCC, Rule Making Process, https://www.fcc.gov/about-fcc/rulemaking-process.