アメリカ合衆国憲法修正四条と プライバシーの合理的期待テスト（1）

葛　　虹

目次

一　はじめに

アメリカ合衆国憲法修正四条は「不合理な捜索及び押収に対して、身体、家屋、書類及び所持品が保障されるという人民の権利は、侵害されてはならず、また、宣誓又は確約により裏付けられた相当な理由に基づいており、かつ、捜索される場所及び逮捕・押収される人又は物を特定して記述するものでなければ、令状は発付されない」と定めている。

アメリカでは、上記条文の第一文は「合理性条項」（the Reasonableness

Clause）と呼ばれ、その第二文は「令状条項」（the Warrant Clause）と呼ばれる。両条項の関係をめぐって、全く別個のものと解する見解と両者が連動するものと解する見解が対立している(1)。後者の見解、令状なしに行った捜索及び押収は、原則不合理だと推定される、つまり連動説は、プライバシー保護に有利な方向に働くと言われる(2)。プライバシーに関する判例においては連動説がほぼ定着している。

実は、実務において法執行行為がいろいろあり、必ずしも令状を必要としない。令状がない場合であっても、必ずしも憲法違反となるわけではない。修正四条にいう「捜索及び押収」に該当するときのみ、憲法違反となる。そして、その該当性をどう判断すべきかが、一番の難所である。

例えば、政府の電子監視行為について、政府が令状なしに電子技術を用いて個人情報を入手する場合、修正四条にいう「捜索」に該当するかどうかを判断する基準が如何なるものべきかよく議論される。「プライバシーの合理的期待テスト」は一応公認の基準として裁判実務で定着したが、絶えず進歩しつつある技術に挑戦され、難しい局面を迎えている。

そもそも、アメリカでは、政府の電子監視活動に関して、電子通信プライバシー法（Electronic Communications Privacy Act、以下「ECPA」と略称する）などの規制がある。これらの規制の役割が果たせない場合は、修正四条の出番となる。そのため、本稿はECPAの規制枠組及びその問題点を検討した後に、修正四条による個人のプライバシー保護の意義について論究する。

二　政府の電子監視行為の法規制

１．ECPAの規制

（1）　ジョシュア・ドレスラーほか著（指宿信監訳）『アメリカ捜査法』（レクシスネクシス・ジャパン、2014）229頁。

（2）　Tracey Maclin, *The Central Meaning of the Fourth Amendment,* 35 William & Mary L.Rev.197 (1993).

1986 年に制定された ECPA は、主に通信傍受法（The Wiretap Act）、通信記録保管法（The Stored Communications Act）、ペンレジスター法（The Pen Register Act）の三つからなる。そのうち、アメリカ国内の一般の犯罪捜査に係る電子監視に関する部分の規制枠組(3)は、以下のようになっている。

捜査対象となる情報は、リアルタイム（Real time）の通信情報と電磁的に保管された (stored) 通信情報に分けて、さらに通信内容情報（contents）と通信外容情報（no-contents、例えば発信時間、電話番号など）に細分する。リアルタイムの通信情報、とりわけそのリアルタイム通信内容情報に対するプライバシー期待が高く、保管通信情報、とりわけその保管通信外容情報に対するプライバシー期待が低いという価値判断により、政府の情報取得に対する規制の内容を決める。

①リアルタイムの通信内容情報の取得について

通信傍受法によれば、法執行官は裁判官が発行した捜索令状（warrant）に基づいて行わなければならない(4)。捜索令状の発行要件は前記修正四条の令状条項に従うことになる。その「相当な理由」の一般的な理解として、単なる容疑（mere suspicion）よりも明確なもので、令状の申請者は、裁判官をして「合理的に信頼できる情報」を把握しており、かつ「それについて通常の注意力を有する人間に、ある犯罪が実施されたか或いは実施されつつあると

（3） アメリカで、国家安全に係る電子監視の規制は、一般の犯罪捜査に係る電子監視の規制と異なる。前者の場合は、連邦調査局（FBI）が自ら発行した国家安全保障書簡（National Security Letter）をもって、第三者の通信会社などに対し、調査対象者に関する電子記録の強制提出を要求することができる。この際、FBI は、次の二点を保証しなければならない。①かかる調査はアメリカ人の単なる合衆国憲法修正 1 条の保障を受ける活動を対象とものではない；②かかる記録はテロや隠れた諜報活動についての合法的な調査と関連していること。また、第三者の通信会社などは、この FBI の調査行為をいかなる者にも告知してはならない。(The Stored Communications Act, 18 U.S.C. § 2709)。本稿の検討はページの都合上、この部分を割愛する。

（4） 18 U.S.C. § 2510-2522.

信じさせるに十分で」あることを確信させなければならない[5]。

さらに、通信傍受法は、違法証拠排除のルールも明記した。「法執行官が法律に違反して情報を収集した場合、情報主体は、それを理由に、違法収集した情報を証拠から排除することを求めることができる」[6]。

②リアルタイムの通信外容情報の取得について

ペンレジスター法によれば、法執行官が裁判所命令（court order）により通信サービス業者の協力を得て、特定の者に対しリアルタイムの通信外容情報の追跡・取得行為を最長60日間にわたり続けることができる[7]。アメリカ法では「裁判所命令」は裁判官が発行するものであるが、その発行要件は各成文法が定める。ペンレジスター法に定めるリアルタイムの通信外容情報の「裁判所命令」の発行要件は、「捜索令状」のものと比べて、非常に緩やかなもので、「現に行われている調査と関連性がある」[8]ことだけである。

③通信サービス業者または遠隔情報処理サービス業者（provider of electronic communication service or remote computing service）に保管された通信内容情報（以下「保管内容情報」と略称する）の取得について

通信記録保管法によれば、保管日から180日以内のものであれば、法執行官は裁判官が発行した捜索令状（warrant）に基づいて行わなければならない。180日を超えたものであれば、法執行官は裁判所命令（court order）ないし召喚状（subpoena）に基づいて行うことができる[9]。

保管内容情報の「捜索令状」の発行要件は、前記①リアルタイムの通信内容情報のものとほぼ同様である。ただし、違法証拠の排除規則は明記されていない。

（5） Brinegar v. United State, 338 U.S.160 (1949).

（6） 18 U.S.C. § 2518 (10) (a).

（7） 18 U.S.C. § 3121-3127.

（8） 18 U.S.C. § 3123 (a).

（9） 18 U.S.C. § 2701-2711.

保管内容情報の「裁判所命令」は、その発行要件が前記②リアルタイム外容情報のものより厳しく、両者を区別するため実務上Ｄ命令（D order）と呼ばれる。通信記録保管法の規定によれば、法執行官は、裁判官に対し、対象通信にかかる内容が進行中の犯罪捜査に関連し重要であることを示す合理的な根拠があることを具体的かつ明瞭な事実（specific and articulable facts）で示す必要があるが[(10)]、「捜索令状」のほど厳しいものではない。

ちなみに、「召喚状」に関しては、ECPA は裁判所の「召喚状」（裁判所の職員が法執行官の申請に基づいて発行するもの）、行政機関の「召喚状」（成文法の授権で法執行官が自ら発行するもの）及び大陪審団の「召喚状」などのいずれのものも認める[(11)]。通常、「召喚状」の発行要件は非常に緩いもので、形式的な関連性などの要件がそろえば、その法的効力が認められる[(12)]。

法執行官は上記の手続に従い保管通信内容情報を取得しなければならないほか、その通信の当事者に対し、事前又は事後の通知を行うという通知義務がある[(13)]。通知された通信当事者が法執行官の取得行為に対し異議を申立できる。

④上記の業者に保管された通信外容情報（以下「保管外容情報」と略称する）の取得について

通信記録保管法によれば、法執行官は、捜索令状又はＤ命令に基づいて、すべての保管外容情報を収集することができる（サービス利用者の氏名、住所、電話番号、利用サービスの種類、支払方法、ID 番号のような保管外容情報だけ収集する場合は、召喚状でも可）。保管内容情報と異なり、法執行官は通信当事者に事前若しくは事後に通知する必要がない[(14)]。通信当事者による

（10）　18 U.S.C. § 2703 (d).

（11）　18 U.S.C. § 2703.

（12）　Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

（13）　18 U.S.C. § 2703 (b) (B). 但し、法執行官が、令状に基づいて保管日から 180 日を超えた情報を入手する場合は、その限りではない (18 U.S.C. § 2703 (b) (A))。

異議申立のチャンスもない[15]。

２．問題の所在

ECPA の通信内容情報と通信外容情報の区別規制の発想は、1877 年の Ex Parte Jackson 連邦最高裁判決に由来したものである。その判旨によれば、封をされた手紙は郵便局に投函された後も、自宅にある書類のように修正四条の保障を受ける。政府による手紙の開封及び内容検査は、令状に相当するものが必要である。ただし、手紙の外見、重量及び封をされた包みを除く[16]。

ところが、21 世紀のインターネット、ビックデータの技術環境の下で、通信内容情報と通信外容情報の区別規制の意義は段々薄くなっている。通信外容情報のみでも、解析可能な量があれば、そこから関係の通信内容情報を読み取ることが可能である[17]。本稿の検討対象である基地局位置情報（cell-site location information）はまさに内容解読可能性をもつ通信外容情報である。

現在の携帯電話は、その発生する電波がその携帯電話会社が設置した基地局によって捕捉されてはじめて通信できるという仕組みになっている。たとえ通信機能を使用しなくても、携帯電話の電源が入った状態であれば、その電波が発生し、最寄りの基地局はそれを捕捉することができる。各基地局は、その捕捉の度に、捕捉時間と場所などの情報（いわゆる基地局位置情報）を自動的に生成し、記録する。その基地局位置情報から携帯電話の使用者の所在地を推測でき、その精度が GPS 情報に近いレベルに達しているといわれる。

個々の基地局位置情報を見る場合は、単なる携帯電話所持者の特定時間帯

（14） 18 U.S.C. § 2703 (c) (3A).

（15） 保管外容情報の場合には、次のような通信事業者による異議申立の規定しか存在しない。法執行官がＤ命令をもって通信事業者にその保管された情報の開示を求める場合は、通信事業者は、かかる情報の提出に過重の負担が課せられるという理由でそのＤ命令に対し異議を申立てることができる (18 U.S.C. § 2703 (d))。

（16） 96 U.S. 727 (1877).

（17） Laura Donohue, *The Dawn of Social Intelligence (SOCINT),* 63 Drake L.Rev.1061(2015).

の所在地を記録したもので、普通の通信外容情報に過ぎない。しかし複数の連続の基地局位置情報の場合は、その携帯電話所持者の日々刻々の動静を記録したものとなり、そこからその者に関するセンシティヴ情報（家族、政治、仕事、宗教、性的関係など）を掘り出すことができる[18]。このように、基地局位置情報、GPS 情報を含む位置情報は単純な通信外容情報とは言えなくなった。

アメリカ連邦議会は、この点について無視しなかった。1994 年に制定された「法執行向け通信支援法」（The Communications Assistance for Law Enforcement Act、以下「CALEA」と略称する）は、法執行官による通信傍受、暗号解読、通信識別情報へのアクセスにおいて、通信事業関係者にその協力・支援を求めるものである[19]。そのなかには、法執行官が裁判所命令をもって、通信事業関係者に対し、そのリアルタイムの通信識別情報の取得に協力するよう要求できる条文があった[20]。この条文の最後には、「加入者の物理的な所在を示す情報（電話番号から判断できる範囲の程度のものを除く）」を適用除外するという文言がついている[21]。ここでいう加入者の物理的な所在を示す情報とは基地局位置情報、GPS 情報などの位置情報を指す。従って、CALEA 成立後、前述したペンレジスター法に定める裁判所命令だけで、リアルタイム基地局位置情報の取得はできなくなった。

また、1999 年に制定された「無線通信及び公衆安全法」（The Wireless

（18） Susan Freiwald, *Cell Phone Location Data and The Fourth Amendment: A Question of Law, Not Fact,* 70 Maryland L.Rev.681 (2011).

（19） 47 U.S.C. § 1002 (a). 具体的にいえば、通信事業関係者はその機器、設備、サービスにおいて、次のような機能を満たすことを保証しなければならない。ⅰ）通信をすみやかに特定し、法執行機関が傍受できるようにすること；ⅱ）通信識別情報をすみやかに特定し、法執行機関がアクセスできるようにすること；ⅲ）傍受した通話内容およびアクセスした発信識別情報を法執行機関へ引渡すことなど。

（20） 47 U.S.C. § 1002 (a) (2).

（21） 47 U.S.C. § 1002 (a) (2) (B).

Communication and Public Safety Act、以下「WCPSA」と略称する）は、通信サービス提供者に対し、携帯電話使用者の位置情報を活用して携帯電話の災害時の緊急通報サービスを承認したほか、1996年の連邦通信法（The Telecommunications Act）の内容の一部を改正し、位置情報に関する特別規定を追加したものである。改立後の連邦通信法によれば、「顧客の独自のネットワーク情報（customer proprietary network information）」、つまり通信サービス提供者がサービス契約に基づいて入手した携帯電話使用者の情報について、通信サービス提供者は、守秘義務があり、法に定める場合又は携帯電話使用者の同意した場合を除き、通信サービスの提供の目的以外に使用、開示などはできない[(22)]。特に、位置情報の目的外の使用に関しては、緊急事態を除き、顧客（携帯電話使用者）の明確な事前の許可がない限り、携帯電話使用者の位置情報の使用、開示又はアクセスの同意と見なさない[(23)]。これと対照的に、ほかの情報の目的外の使用に関しては、このような特別規定がない。すなわち、顧客の位置情報の目的外使用の同意要件は、顧客のほかの情報より厳しく設定される。この点からも、位置情報に対する特別扱いの立法意図を読み取れる[(24)]。

とはいえ、CALEA、WCPSAないし改正後の連邦通信法のいずれも、法執官による位置情報の取得についてさらに一歩踏み込んだ規制を明示しなかった。そのため、実務では、法執行官は依然としてECPAの規定に従い基地局位置情報を入手することになる。ただ、CALEAのリアルタイム位置情報の適用除外の規定があるので、リアルタイム基地局位置情報を取得しようとする法執行官は、この規定をクリアする必要がある。そして、彼らはハイブリッド命令というものを創出した。つまり、ECPAの通信記録保管法[(25)]及びペン

(22) 47 U.S.C. § 222 (c) (1).

(23) 47 U.S.C. § 222 (f) (1).

(24) Susan Freiwald & Stephen Smith, *The Carpenter Chronicle: A Near-Perfect Surveillance,* 132 Harv.L.Rev.205 (2018).

レジスター法[26]に定めた発行要件の両方を満たす最長 60 日間のＤ命令によってリアルタイム基地局位置情報を取得するという対策であった。下級裁判所は最初、このような対策を認めた。

しかし、2005 年以降、一部の下級裁判所は、ハイブリッド命令そのものが法的根拠を欠くという理由で、ハイブリッド命令の発行申請を拒否した[27]。以後、リアルタイム基地局位置情報の取得には捜索令状が必要であるという考えは一般的になった[28]。

ところが、実務ではまた新たな対策が考え出された。一部の法執行官は ECPA の通信記録保管法の規定[29]を利用し、Ｄ命令を申請することによって、リアルタイム基地局位置情報の代わりに、その数日後のものすなわち保管基地局位置情報になったものを入手するという対策であった。このやり方は、令状の抜け道だと学者らに批判された[30]。前述したように、ECPA の通信記録保管法に定めるＤ命令の発行要件が令状より緩いのみならず、係る保管基地局位置情報が単なる保管外容情報と扱われ、その取得際の情報主体への通知規定がなく、情報主体による異議申立の機会も保障されないので、情報主体のプライバシーへの侵害リスクが高いと懸念された。

これらの問題の根本解決には、やはり ECPA の抜本的な改正が必要である。しかし、連邦議会では ECPA の法改正案がなかなか可決できなかった[31]。そ

（25） 18 U.S.C. § 2703 (d).

（26） 18 U.S.C. § 3123 (c) (1).

（27） E.g., *In Re* Application for Pen Register and Trap/Trace, 396 F. Supp. 2d 747,754 (S.D. Tex. 2005); *In Re* Application of the U.S. for an Order Authorizing (1) Installation and Use of a Pen Register and Trap & Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F.Supp.2d 816,827-36 (S.D.Tex.2006).

（28） Susan Freiwald & Stephen Smith, *supra* note 24, at 213.

（29） 18 U.S.C. § 2703 (d)

（30） Susan Freiwald & Stephen Smith, *supra* note 24, at 213.

（31） E.g., ECPA Modernization Act of 2017, S.1657, 115th Cong.

して、個別事案の当事者の救済のため、修正四条が最後の砦として登場した。

三　電子監視活動に関する従来の修正四条判例法理

1「物理的侵入法理」から「プライバシーの合理的期待テスト」へ

1960 年代以前、連邦最高裁は、修正四条にいう「捜索」について、法執行官は捜査対象者の家、土地に無理やりに侵入し、くまなく捜し回るという捜査手法を想定していた。そのため、私的空間への物理的侵入があるかどうかを焦点とする「物理的侵入法理（The Physical Trespass Doctrine）」を判断基準とした判例が多く見られた。

例えば、Olmstead v. United States(32) 判決では、法執行官は捜査対象者の個人専用オフィスなどから出ている普通電話線にワイヤーを取りつけ、その電話を盗聴することで、その犯罪事実を掴むという捜査手法が修正四条に違反するかどうかが問われた。

連邦最高裁の多数意見は、「物理的侵入法理」を判断基準とし、その盗聴行為が私的空間への物理的侵入を伴わないとして、修正四条にいう「捜索」に該当しないと結論づけた。これに対し、Brandeis 裁判官はその反対意見において、多数意見の保守的な考えを批判し、技術の進歩に相応するより柔軟で進化的なアプローチをとるべきであると指摘した。

こうした流れは、1967 年の Katz v. United State(33) 判決によって変えられた。賭博技術のプロである Katz は、公衆電話を利用して賭博に関する情報を関係者へ有料提供したことで刑事起訴された。FBI の捜査官は令状に基づかずにその公衆電話ボックスの外側に盗聴録音機を取り付けたことによって取得した Katz の会話記録を、裁判で証拠として提出した。これに対し、Katz は、FBI の行為が連邦憲法修正四条に違反したと主張し、その証拠について、排

(32)　277 U.S. 438 (1928).

(33)　389 U.S. 347 (1967).

除の申出（motion to suppress evidence）をした。

連邦最高裁の多数意見は、従来の「物理的侵入法理」を採用せず、「修正四条は、場所ではなく、人を保護している。…人がプライベートなものとして保持しようとした事柄は、公衆にアクセス可能な領域の中であったとしても、憲法上の保護を受ける可能性がある」と述べ、本件の捜査手法が連邦憲法修正四条にいう捜索に該当し、本件の無令状捜索が連邦憲法修正四条に違反すると判断した。結果として、Katz の証拠排除の申出を認めた。

上記の多数意見の補足として、Harlan 裁判官はその同調意見で、次のように述べた。「私は上記決定から生まれたルールについて二つの要件が含まれると理解している。一つは、個人が実際の（主観的な）プライバシーの期待を示したということである。もう一つは、その期待を社会が合理的であると認めることである。」

Katz 判決は、大きな社会反響を呼んだ。以降、公衆にアクセス可能な領域に居ても個人がそのプライバシーをすべて失うわけではないという考え方は定着した。又、Harlan 裁判官の２要件の論述は「プライバシーの合理的期待テスト」と呼ばれ、修正四条にいう捜索に該当するかどうかを判断する公認の基準となった。

２　新技術環境の下での問題点

「プライバシーの合理的期待テスト」をめぐって、そのはじめから賛否両論があった。技術の進歩、社会の変化に柔軟に対応できると評価された一方、他方において「何がプライバシーの合理的期待であるか」についての具体的な指標を示せず、「一種の循環論法に陥っている」と批判された(34)。

また、「このテストは、その定式化の方法からして、プライバシーに関する

(34)　Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court,* 1979 Sup. Ct.Rev.173 (1979).

社会的見解の経験的な測定基準であるとされている。しかし、最高裁は、社会が合理的なものとして扱っているプライバシーの期待が何かについての結論を支持するために、経験的証拠を引用することはなかった」[35]。その原因について、学者らは以下のように指摘した。

そもそも、社会におけるプライバシーの合理的期待そのものの測定が非常に難しい。裁判所は組織面、資金面などにおいて、大衆の習慣及び傾向に関する調査を行うに必要な人力、財力を備えていない[36]。そのため、このような調査を避けてきた。

また、仮に社会におけるプライバシーの合理的期待は測定できるとしても、その結果はあくまでも多数者の意見を反映したものである。裁判所はその結果を基準とする場合は、少数者の意見を無視してしまい、憲法による人権保護の目的に反するリスクがある[37]。

結局、以下の判例のように、「人や社会がどう期待するかについて、客観的な手法で決定することができず、結局裁判官の主観的な評価に高度に依拠してしまった」[38]。

---

(35) ダニエル･J･ソロブ（赤坂亮太ほか訳）『プライバシーなんていらない !?』（勁草書房、2017）131 頁。

(36) William Baude & James Y.Stern, *The Positive Law Model of the Fourth Amendment,* 129 Harv.L.Rev.1852 (2016). 具体的な難点として、「調査の範囲をどこまでしたらよいかわからない」、「このような調査に必要な費用は低くない」、「裁判所のペースに合わせるため大量な調査が行なければならない」、「裁判官はどの事実が大衆の期待を左右する事実かとの判断が苦手であるため、案件に係る事実の文脈における一見小さな変更が起きても、新たな調査を行うだろう」を挙げた。

(37) ソロブ･前掲書（注 35）131 頁。「多くの論者は、最高裁が社会の実際のプライバシーの合理的期待を無視していることを批判してきた。しかし、最高裁が社会の実際の期待に目を向けなかったことには十分な理由がある。最高裁が投票や世論調査の結果に従うとしたら、修正四条を多数派の選好に縛り付けることになってしまうだろう。少数者の集団は、プライバシーに関して異なる意見をもっているかもしれない。そして、憲法の目的は、多数者の意思を制約して少数者を保護する点にある。」

① California v. Greenwood 判決[39]。警察官が犯罪被疑者の自宅前の公共道路の縁石に置かれたごみ袋の中身を捜査する行為に対し、連邦最高裁は、捨てたものに対しプライバシーの合理的期待が存在しないと判断した。

② Florida v. Riley 判決[40]。警察はヘリコプターに搭乗し、被告人の温室の上空 400 フィートの高度で飛行させ、温室の屋根の欠けている箇所から温室の中で大麻を栽培していることを発見した。連邦最高裁は、ヘリコプターからその温室の内部が見られないという被告人の合理的期待が存在しないと判断した。

③ United States v. Knotts 判決[41]。警察が業者の協力で Knotts の車にのせたコンテナにビーパーをつけて、公道でそのビーパーの信号に頼って Knotts の車に一日尾行したことに対し、連邦最高裁は、公道で車を走らせる者が自分の行動にプライバシーの合理的な期待が存在しないと判断した。

1992 年、Christopher Slobogin 教授（法学）と Joseph Schumacher 教授（心理学）は、1967 年の Katz v. United State 判決から 25 年間の連邦最高裁の「プライバシーの合理的期待テスト」に関する判断が、社会の実際のプライバシーの合理的期待と合致するかどうかについて、社会調査を行った。彼らは、捜索・押収に係わるプライバシーへの侵入感覚の程度を 0 ～ 100 で測り、0 を「全く感じられない程度」、100 を「侵入程度が極端に感じられた」と表記した。彼らの調査結果としては、Florida v. Riley 判決は 40.32、California v. Greenwood 判決は 44.95、United States v. Knotts 判決は 54.46、後述する United States v. Miller 判決[42] は 71.60 であった。彼らの結論によれば、中間値 50 を

(38) Amital Etzion, *PRIVACY IN A CYBER AGE: POLICY AND PRACTICE* 23-24 (Palgrave Macmillan, 2015).

(39) 486 U.S.35 (1988).

(40) 488 U.S.445 (1989).

(41) 460 U.S.276 (1983).

(42) 425 U.S.435 (1976).

社会の実際のプライバシーの合理的期待を引起す標準値とすれば、連邦最高裁の判断は、必ずしも社会一般の感覚と一致していない[43]。

3　第三者提供法理

連邦最高裁はプライバシーの合理的期待テストに対する批判を意識しながら、その規範的な適用の実現に工夫した。それは、除去法を用いて、「何がプライバシーの合理的期待であるか」という問題への直接な回答を避けて、とりあえず適用外対象を明確にするという「第三者提供法理」の創出である。この法理は、以下の二つの判例に由来した。

① United States v. Miller 判決[44]。密造酒の取締を担当する政府職員が文書提出命令に基づいて銀行から Miller の口座情報を入手したが、銀行はそのことを Miller に知らせなかった。連邦最高裁は、Miller が自由意思で関係情報を銀行に伝えた以上、その関係情報が銀行から政府へさらに伝われるリスクを負うので、その口座情報に対する合理的期待が存在しないと判断した。

② Smith v. Maryland 判決[45]。警察は、強盗犯罪容疑者を特定するため、電話会社で通話先探知機（pen register）を令状に基づくことなく設置し、Smith の自宅から発信したすべての電話番号を記録した。連邦最高裁は、電話使用者が電話会社に通話先の電話番号を伝え、電話会社の交換機を経由して通話すること、およびこれらの電話番号が電話会社に記録されることが一般的に知られる事項で、たとえ Smith のようにこれらの電話番号の秘密性に対し強い主観的期待を持つ者がいても、このような期待は社会通念に照らして受け入れるものではないと判断した。

（43） Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 Duke L.J.727 (1993).

（44） 425 U.S.435 (1976).

（45） 442 U.S.735 (1979).

要するに、第三者提供法理は、個人は、自分に関する情報を第三者に任意提供した以上、その情報に対する合理的期待を有しておらず、その結果、修正四条の保護を受けることができないとの判例法理である。その背後には「リスク引受け法理」（そもそも秘密捜査官、秘密情報協力者の捜査参加によって得た情報を犯罪の証拠として使えるかという問題に対処する判例法理）(46) が論拠とされている。つまり、個人が他人に対し、秘密を打ち明けた以上、他人の裏切りのリスク (misplaced trust) を引き受けなければならないという考え方である。

これに対し、Solove 教授は、情報主体本人による提供の任意性ではなく、第三者による再提供の任意性に着目し、上記の論拠について「不適切だ」と批判した。この二つの法理は「類似したものではない。誤って信頼した友人に裏切られた場合（あるいは秘密捜査官の場合）、友人（秘密捜査官）は、自らの意思であなたの秘密を開示することを選択している。しかし、多くの場合、銀行や電話会社は自らの意思で顧客の情報を開示することを選択していない。それらの企業は政府によって顧客の情報を開示するように強いられているのである。実際、それらの企業はしばしば顧客の秘密を保持したいと思っている」(47)。

特に、情報共有が常態化している情報社会における第三者提供法理の適用の妥当性について、疑問視する声は一段と大きかった。

「情報時代において、前例のない規模のパーソナルデータが様々な企業や組織により管理されている。ケーブルテレビ会社はあなたの視聴した映画やテレビ番組の記録を保有している。電話会社はあなたが電話したあらゆる相手

（46） Hoffa v. United States 判決（385 U.S.293 (1966). 秘密情報協力者が捜査対象者 Hoffa の友人になりすまして彼から贈賄の情報を収集した事件）及び Lewis v. United States 判決（385 U.S.206 (1966). 捜査対象者は秘密捜査官を自宅に招いて麻薬の取引を行った事件）. 連邦最高裁は、両事件とも修正四条に反しないと判断した。

（47） ソロブ・前掲書（注 35）120 頁。

の番号に関するデータを保有している。消費者報告機関は、あなたの住所、金融機関の口座、債務の返済履歴に関するデータを保有している。病院や保険会社はあなたの健康情報を保有しているし、クレジットカード会社はあなたの購買履歴を保有している。」「それだけではない。フェイスブックに登録している人は、友人にしか見せたくない大量のプロフィール情報をあげているかもしれない。グーグルはあなたの一定期間内のすべての検索履歴を保有している。アマゾン・ドットコムのような販売サイトはあなたの購買記録のすべてを保有している」(48)。

もし第三者提供法理に従えば、これらの第三者に保有されるデータ、記録に対し、情報主体のプライバシーの合理的期待はすべて認められないことになる。そして、情報技術の発展に伴い、情報共有が進むなか、第三者提供法理を堅持すべきかという問題をめぐって、学者の間には激しい論争があった。

擁護派の代表 Kerr 教授の観点は以下のようにまとめることができる。第三者提供法理は、第三者への開示の時点でプライバシーの期待が消滅するという理屈を採用するため、明確性、予測可能性が高いというメリットがある(49)。新情報技術の発展に伴い犯罪能力が向上しつつある現状の下で、第三者提供法理の適用によって法執行機関の権限を拡大させてしまうという結果が生じても、それは犯罪能力の向上に相応するための権限の拡大で、不合理的なものではない(50)。

これに対し、反対派の代表 Solove 教授は、「第三者提供の法理のもとで、政府は今やあなたの自宅に入らなくても、あなたについて多くのことを調べあげることができる。…」「したがって、政府は、修正四条の保護の及ばないそれらの情報すべてを入手できる。デジタル時代において、修正四条はしだいに意味を失いかけており、政府は、ほとんどいかなる監督や制限に服する

（48） ソロブ・前掲書（注 35）113 ～ 114 頁。

（49） Orin S. Kerr, *The Case for the Third-Party Doctrine,* 107 Mich. L. Rev. 581-586 (2009).

（50） *Id*. at 579-581.

ことなく、あなたの情報にアクセスできるようになっている」[51] と批評した。さらに、最高裁が第三者提供法理の射程を明確に示さないせいで、第三者提供法理が広汎に適用される可能性があり、その結果、修正四条の保障が事実上台無しになってしまうおそれがあると指摘した。

Neil M. Richards 教授も、第三者提供法理の広汎な適用について同様な懸念を持ち、特にクラウドで保存されている電子文書にまでその適用を広げる傾向に強く警戒している。彼の見解によれば、United States v. Miller 判決と Smith v. Maryland 判決から導かれた第三者提供の法理は、本来「極小の第三者提供法理」（Tiny of Third-Party Doctrine）であるはずだったが、その射程が曖昧なため、現在「広義的な読みの第三者提供法理」（broad reading of Third-Party Doctrine）と理解されてしまった。このまま放置すれば、クラウドのようなデジタル世界では、プライバシーがこの「広義的な読みの第三者提供法理」に呑み込まれ、法的保障が得られなくなってしまう結果になる[52]。そのため、彼は「広義的な読みの第三者提供法理」という考えについて一定の歯止めをかけるべきであると主張した[53]。

ほかにも第三者提供法理を批判した学者が多数いる[54]。又、アメリカの一部の州裁判所（e.g. New Jersey 州、Colorado 州、California 州、Florida 州、Hawaii 州、Illinois 州、Idaho 州、Montana 州、Pennsylvania 州、Utah 州、Washington 州）[55] も、以前から州憲法の規定に反するという理由で、法執行官による銀行記録、電話記録などの第三者からの入手行為に対し、第三者提

（51）　ソロブ・前掲書（注 35）114 頁。

（52）　Neil M. Richards, *The Third-party Doctrine and The Future of Cloud,* 94 Washington L.Rev.1466-1475 (2017).

（53）　*Id.* at 1442.

（54）　E.g., Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data,* 14 J.L.& Pol'y 211 (2006); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expections,* 24 Berkeley Tech.L.J.1199 (2009).

供法理の適用を拒否してきた(56)。そして、ついに、連邦最高裁の Sotomayor 裁判官も後述する United States v. Jones 判決での同調意見において、反対派に近い見解を以下のように示唆した。

「情報が自発的に第三者に開示された場合、個人はプライバシーの合理的な期待を有しないという前提を再考する必要がある。このアプローチはデジタル時代には適合しない。人々は、自分の任務を実行する過程で自らの情報を多く第三者に開示するからである。…修正四条が秘密をプライバシーの前提条件として扱うことを停止しない限り、彼らは憲法上の保障を得ることができない。私は、限定的な目的で一部の公衆に開示した情報のすべては、この（開示の）理由だけで、修正四条の保障を失ってしまうと考えていない」(57)。

このように、第三者提供法理が時代の変化に応じ、見直されなければならない局面を迎えた。

4　モザイク理論

前述した情報共有の問題のほか、学者らは、情報社会のもう一つの問題にも注目している。それは、情報技術の飛躍的な発展に伴い、公共の場での広範囲かつ大規模な監視が容易となり、この種の監視によって得た情報は、プロファイリング、データマイニング、照合（matching）などのデータ処理技術によって処理された後、個人のプライバシーに深く関わる情報に変身しうるという問題である。しかし、従来の判例法理（e.g. United States v. Knotts 判決(58)）によれば、この種の監視によって得た情報は公道での情報で、はじめ

（55） Stephen Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogues to Protect Third Party Information from Unreasonable Seizure,* 55 Cath. U.L.Rev.395 (2006).

（56） E.g., State v. Hunt, 450 A.2d 952 (N.J. 1982) ; Winfield v. Div. of PariMutuel Wagering, 477 So. 2d 544, 548 (Fla. 1985).

（57） 565 U.S. 400, 416 (2012).

（58） 460 U.S.276 (1983).

から個人のプライバシーの合理的期待が認められない。この流れで、データ処理技術にかけられ変身した情報にも個人のプライバシーの合理的期待が認められない。このままにすると、深刻なプライバシー侵害結果が生じかねない。この問題に対処するため、新たな法理を探す必要がある(59)。

こうして、「モザイク理論」が注目を集めることとなった。それは、一見価値があまりない断片的な情報が、多数集約され、その相関関係が明らかになり、その相乗作用によって、個々の情報の総体以上の価値を有する情報のモザイクが生み出されるという考え方である。以前から、アメリカの連邦情報公開法（Freedom of Information Act, 以下「FOIA」と略称する）に定める国防又は外交政策に係る情報の適用除外の規定(60) に対する解釈において採用されたものである(61)。

修正四条に係る裁判ではじめて「モザイク理論」に言及したのは、コロンビア特別区連邦控訴裁判所の United States v. Maynard 判決である。それは、警察が有効な令状に基づかず 28 日にも及ぶ GPS の監視を行った行動が捜索に該当するかどうかが問われる事件である。

Ginsburg 連邦控訴裁判官はその判決文で「政府が国家安全保障に関する案件においてしばしば持ち出す『モザイク理論（mosaic theory)』と同様に、情報をもたない者にとっては些細なものように見えるものは、広い見識を持つ者にとっては素晴らしいものと見えるかもしれない。…長期間の監視により、人が繰り返し行うこと、行わないこと、アンサンブルすることなど、短期間

---

(59)　Helen Nissenbaum, *Protecting Privacy in the Information Age: The Problem of Privacy in Public,* 17 Law & Phil.559 (1998).

(60)　5 U.S.C. § 552 (b) (1) (A).

(61)　David Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act,* 115 Yale L.J.628 (2005). 政府は国防又は外交政策に係る情報の開示が請求された事案においては、請求対象となる情報の一つ一つが国家安全保障を直接害する情報ではなくても、それらを繋ぎあわせることにより、国家の安全保障を脅かす重大な情報になりうる可能性がある場合には、その開示請求を認めないことができる。

の監視では明らかにされない種類の情報が明らかになる」[62] と書き、警察の長時間の公道での GPS 捜査が修正四条の捜索に該当すると判断した。

United States v. Maynard 判決の上告は認められた。上告審である United States v. Jones 判決のなかでは、Alito 裁判官はその結論同調意見でモザイク理論について明確に言及しなかったが、原審の Ginsburg 連邦控訴裁判所裁判官と同様な問題意識を表明した。Alito 裁判官の意見によれば、United States v. Knotts 判決のように車の公道での動きについて短期間監視（short-term monitoring）を行うことは社会通念上認められるプライバシーの合理的期待に反しないが、本件のような長期間の監視（longer-term monitoring）はプライバシーの合理的期待を害する[63]。

また、Sotomayor 裁判官がその同調意見において、Alito 裁判官の「長期間の監視はプライバシーの合理的期待を害する」との観点に賛同し[64]、長期間の GPS 監視によって蓄積された情報から、個人の家族関係、政治的繋がり、専門家たちとの繋がり、宗教上の繋がり、性的関係の詳細を炙り出す可能性があると指摘した[65]。

その結果、Alito 裁判官の結論同調意見は連邦最高裁の法廷意見ではないが、Sotomayor 裁判官を含む事実上過半数（５名）の裁判官の支持を得た。そのため、一部の学者がこれらの裁判官の意見をまとめて「修正四条のモザイク理論」（the mosaic theory of the fourth amendment）と呼ぶようになった[66]。

その後の Riley v. California 訴訟[67] は、逮捕時における被逮捕者の携帯電話の無令状捜索の可否を争った事件である。同様な問題意識を持つ連邦最高裁

（62） 615 F.3d 544 (D.C.Cir.2010).

（63） 565 U.S. 400, 430 (2012).

（64） 565 U.S. 400, 414 (2012).

（65） 565 U.S. 400, 415 (2012).

（66） Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment,* 111 Mich.L.Rev.325 (2012).

（67） 573 U.S. 373 (2014).

Roberts 長官が執筆した法廷意見は、上記 Sotomayor 裁判官の意見を引用しながら、次のように述べた上で、ノーという結論を下した。

「携帯電話は被逮捕者が所持する他のものとは質・量共に異なる…」[68]。「現代の携帯電話の最も際立った特徴の一つは、その巨大な蓄積能力である。携帯電話の蓄積能力はプライバシーと相関関係がある。第一、携帯電話は一箇所でも様々な情報を収録し──住所、覚書、処方、銀行取引明細、録画──その組み合わせにより、個別の記録からは知ることができない事実を明らかにする。第二、たとえ一種類の情報でも、伝えられるものが以前より遥かに多い。（ある者に関する）日付、場所及び説明がついた写真千枚をまとめれば、その者の私生活を再現することができる。財布のなかに挟んだ愛する人の写真１枚２枚で同様なことを語ることはできない。第三、携帯電話のデータは購入時ないしもっと遠い過去まで遡ることができる…」[69]。

「携帯電話に蓄積されたデータは、単に量的な面において物理的な記録と比べて桁違いであることにとどまらず、質的な面においても一定種類のデータが特異性を有する。例えば、インターネット機能付きの携帯電話のなかから見つけたインターネット上の検索、閲覧履歴は、個人の私的利益又は関心を明らかにさせることができる。──多分一回の病気症状の検索も、WebMD(訳者注：アメリカの医療情報サイト) の頻繁訪問という事実につなぐことになる。携帯電話のテータは個人の所在を明らかにすることができる。位置情報の履歴は多くのスマートフォンの標準搭載で、街にとどまらず、特定建物のなかにいるある個人の特定の動きを分単位で再現することができる」[70]。

このように上記二件の連邦最高裁判例によって、「モザイク理論」が一躍注目された。とはいえ、Alito 裁判官の結論同調意見が厳格な意味での「モザイク理論」ではないとの指摘がある[71]。Alito 裁判官は明らかに監視という情報

(68)　573 U.S. 389 (2014).

(69)　573 U.S. 390 (2014).

(70)　573 U.S. 391 (2014).

取得行為だけを問題視しているからである。それと対照的に、Sotomayor 裁判官の意見は、長期間の監視（情報の取得行為）にとどまらず、その後の蓄積、結合の行為も問題視している。この意味では、確かに Sotomayor 裁判官の意見は「モザイク理論」に近いものといえる。

それにもかかわらず、アメリカでは Alito 裁判官の「長期間の監視はプライバシーの合理的期待を害する」という考え方を含む「モザイク理論」と見なす学者が少なくない。この理論の是非をめぐって以下のような論争もあった。

Kerr 教授[72] は、「修正四条のモザイク理論」がプライバシーの合理的期待テストの重大な軌道修正であると指摘した。彼の見解によれば、従来は政府行動を一つ一つ見て、そのなかからプライバシーの合理的期待に反し、修正四条にいう捜索に該当するものがあるかどうかを判断するが、Alito 裁判官の考え方は政府の一連の行動を結合して全体として捉え、修正四条にいう捜索の程度に達するかどうかを評定する。しかし、この考え方には線引きの問題がある。どの基準でどの時点でプライバシーの合理的期待のラインを超えたと言えるか明らかになっていない。「もし 28 日間が長すぎたら、21 日間はどうですか、14 日間はいかがですか、あるいは 3.6 日間は？ラインはどこにありますか？」[73] Kerr 教授の結論としては、この考え方は基準が曖昧すぎ、下級審ないし現場の警察官に大きな混乱をもたらしてしまうので、採用すべきではない。

これに対し、Etzion 教授は、Kerr 教授と異なる見解をもつ。「法律上、このような線引き問題は多数存在する。例えば、容疑者が起訴または釈放されるまでに拘留される日数、選挙権や運転免許の年齢、デュープロセスに必要な

(71) 尾崎愛美「アメリカの GPS 捜査とプライバシー保護」指宿信編著『GPS 捜査とプライバシー保護』（現代人文社、2018）111 頁。

(72) Kerr, *supra* note 66, at 325.

(73) *Id.* at 333.

陪審員の数等々。…現実の運用では、それが明らかに行き過ぎているのか、あるいは不十分なのかの妥協案として、裁判官が考慮したものを反映している──この線引きはつねに調整できる。集められた情報のボリュームが同様に決められるべきではない理由はない」[74]。

総じて、モザイク理論は、ビッグデータ技術の発展によってもたらされた新たな問題に焦点を当て、content/non-content の分類を打破し、情報の量、情報の結合程度などを重要視することによって、従来プライバシーの合理的な期待が認められない情報まで保護の範囲が広がるという点で評価できる。ただ、個人情報保護の分野では、この理論はまだ学術討論のレベルにとどまり、裁判実務で定着していない。やはり、線引き問題はこの理論のネックであろう。

四　Carpenter v. United States 連邦最高裁判決[75]

2018 年の Carpenter v. United States 判決は、基地局位置情報に関するはじめての連邦最高裁判決、ないし第三者提供法理の適用にはじめて歯止めがかけられた連邦最高裁判決として注目されている[76]。この事件そのものは、前述した情報共有の常態化に伴って生じた問題と公共の場での監視に伴って生じた問題の両方を抱えており、高度情報化社会におけるプライバシー保護の研

(74)　Etzion, *supra* note 38, at 23.

(75)　138 S.Ct.2206 (2018). この判決に関する日本の先行研究として、中曾久雄「携帯電話の位置情報とプライバシー①」地域創成研究年報第 14 号 20 頁（2019 年）、中曾久雄「携帯電話の位置情報とプライバシー②」愛媛大学教育学部紀要第 66 巻 101 頁（2019 年）、緑大輔「携帯電話会社基地局に蓄積された被疑者の位置情報履歴を捜査機関が無令状で取得した行為が違憲と判断された事例」判例時報 2379 号 128 頁（2018 年）、尾崎愛美・亀井源太郎「基地局位置情報取得捜査と令状の要否」情報法制研究第 4 号 15 頁（2018 年）、海野敦史「プライバシーの合理的な期待」の法理の限界からみた監視型情報の収集との関係における憲法上のプライバシー保護のあり方」情報通信学会誌第 36 巻 4 号 63 頁（2018）などがある。

(76)　Paul M. Schwartz, *Legal Access to the Global Cloud,* 118 Colum.L.Rev.1711 (2018).

究に供する絶好な素材である。また、この判決で表われた連邦最高裁の裁判官の間の意見対立も興味深いもので、修正四条とプライバシーの合理的期待テストの関係及び今後のなりゆきをめぐるアメリカでの議論を窺うことができる。

1　事件の経緯

FBI が通信記録保管法の規定[77] にしたがって裁判所から発行されたD命令に基づいて、二つの携帯電話会社から、Carpenter の携帯電話の保管基地局情報計 12,898 個（それぞれ 127 日間分と２日間分）を入手した。そこから析出した一部の情報を Carpenter が犯罪現場の近くにいた証拠として法廷に提出した。Carpenter は、FBI が令状によらず上記の情報を取得した行為が修正四条に反するという理由で、違法に収集した証拠について排除の申立てをした。

保管基地局位置情報は携帯電話会社の設備が記録、蓄積されたものである。下級審の裁判官らは従来の第三者提供法理により、その保管基地局位置情報に対する Carpenter のプライバシーの合理的期待を認めず、その証拠排除の申立を棄却した。Carpenter は連邦最高裁に上告し、その審理が認められた。

結果として、連邦最高裁は、５対４の多数決で Carpenter の主張を是認し、原審を破棄し、差し戻した。この判決には Roberts 長官が執筆した法廷意見（Ginsburg 裁判官、Breyer 裁判官、Sotomayor 裁判官、Kagan 裁判官同調）のほか、Kennedy 裁判官、Thomas 裁判官、Alito 裁判官及び Gorsuch 裁判官がそれぞれ書いた反対意見がある。

2　法廷意見

法廷意見は、先ず、以下のように前例と比較しながら FBI による Carpenter の基地局情報の入手という行為の私生活への侵入性を検討し、「プライバシー

(77)　18 U.S.C. § 2703 (d).

への懸念がより大きい」と判断した。

「Knotts 事件におけるビーパーが装着されたコンテナや Jones 事件における車両と異なり、携帯電話は──まるで人体の一部のように──使用者の動静を完璧に近いほど正確に追跡する。個人は車両からは度々離れるが、携帯電話からはいつも離れることなく所持している。携帯電話は、忠実にその所有者の後について、公道から個人住所、病院、政党本部、その他暴露可能の場所まで往来する。…よって、政府が携帯電話の位置を追跡するとき、携帯電話使用者の足首に監視装置を装着したかのように、完璧に近いほどの監視ができる」(78)。

「携帯電話を用いた追跡は、伝統的な捜査手法と比べ特に容易かつ安価で効率的である。ボタンをクリックするだけで，政府は，実質的な負担なく、（携帯電話会社に）保管された個々の使用者の深い過去の位置情報にアクセスすることが可能となる」(79)。

「アメリカ国内にある 4 億台の携帯電話の位置情報は絶え間なく記録されている。この新たに発見された追跡機能は──たまたま捜査視野に入った者のみならず──全ての人物に対し実施できる。Jones 事件の GPS 装置と違い、警察が特定の個人を追跡するか否か、いつ追跡するかを事前に認識する必要はない」(80)。

「被疑者誰でも五年間の日々の動静が事実上追跡されうる。警察は──政府の見解によれば──修正四条の制約を受けず、かかる監視の成果を求めることができる。携帯電話を捨てない限り、この絶え間ない完璧な監視から逃れられる者はほとんどいない」(81)。

そして、法廷意見は、以下の理由で第三者提供法理の適用を否定した。

---

(78)　138 S.Ct.2206, 2218 (2018).

(79)　*Id.*

(80)　*Id.*

(81)　*Id.*

基地局位置情報のセンシティヴ性は United States v. Miller 判決のビジネス記録及び Smith v. Maryland 判決の電話番号と比べてまったく違う種類のものである。「127 日間の携帯電話の位置記録の調査によって、使用者の位置に関する全方位記録が浮上する。GPS 情報と同様、この種のタイムスタンプ情報は、個人の生活をのぞく秘密の窓のように、個人の個別の動静のみならず、『家族, 政治, 仕事, 宗教, 性的関係』（…Sotomayor 裁判官の観点）(82) を明らかにする。これらの位置記録は、多数の国民にとって『生活に関するプライバシー』（Riley 判決、573 U.S., at _, …）(83) と考えられている」(84)。

また、第三者との共有の面においても使用者の明確な意思によらず、携帯電話の自動装置によるもので、厳密な意味における任意提供とはいえない(85)。

総じて、法廷意見は、FBI が令状なしに Carpenter に関する基地局情報を入手した行為が修正四条にいう「不合理的な捜索」に該当し、憲法違反とした。

3　反対意見

反対した四人の裁判官はそれぞれに自分なりの反対意見を書いた。その分量は合わせて全判決文の三分の二以上を占めた。その内容は以下のように非常に示唆に富むものである。

① Kennedy 裁判官の反対意見（Thomas 裁判官、Alito 裁判官同調）は、修正四条に保護されるプライバシー利益の有無が財産を基礎とする概念（property-based concept）に基づいて判断すべきであると主張した。

彼の意見によれば、本件の基地局位置情報はあくまでも携帯電話会社のも

(82)　原文のままで引用した。United States v. Jones 判決（565 U.S.400, 415 (2012)）の Sotomayor 裁判官の同調意見を指す。

(83)　原文のままで引用した。Roberts 長官が Riley v. California 判決（573 U.S., (2014)）で執筆した法廷意見を指す。

(84)　138 S.Ct.2206, 2217 (2018).

(85)　138 S.Ct.2206, 2218 (2018).

のである。連邦通信法（47 U.S. Code § 222）は携帯電話の加入者に対し関係情報の一定のアクセス権利を認めるが、コントロールの権利としては認めないため、Carpenter は本件の基地局位置情報に対する財産を基礎とする概念上の権益を有せず、Carpenter のプライバシーの合理的な期待を認めることができない[86]。

② Thomas 裁判官はプライバシーの合理的な期待テストを完全否定し、修正四条の原意に従って解釈すべきであると主張した。

彼は「本件では、捜索が生じたか否かという問題に焦点をあてるべきではない。むしろ、誰の財産が捜索されたかに焦点をあてるべきである」[87] と指摘したほか、修正四条の保障対象となる財産はプライバシー、他人の財産というものまで拡大すべきではなく、文字通り個人の「家屋、書類及び所持品」に限定すべきであると言った。その結論として、本件の基地局位置情報が電話会社の財産であるため、Carpenter は修正四条の保護を求めることができない。

③ Alito 裁判官の反対意見（Thomas 裁判官同調）によれば、通信記録保管法には、法執行機関が裁判所命令に基づいて通信記録保管者（携帯電話会社）に顧客の外容情報（基地局位置情報）の提出を命じる際に、通信記録保管者（携帯電話会社）の異議申立手続の定めがある[88] が、顧客の異議申立手続の定めがない。この顧客の異議申立手続を与えるべきかどうかの問題解決は、本来なら、立法機関に任せるべきであるが、法廷意見は新技術による個人のプライバシーへの影響を懸念するという理由で、あえて修正四条に定める令状要件を本件に適用し、Carpenter の証拠排除の申立てを認めた。しかし、このような強引なやり方が修正四条の本意に反し、従来の判例法に混乱をもたらしたほか、立法機関による通信記録保管法の抜本的な改正の意欲もそこなって

(86)　138 S.Ct.2206, 2223-2224 (2018).

(87)　138 S.Ct.2206, 2235 (2018).

(88)　18 U.S.C. § 2703 (d). 本件の場合は、携帯電話会社はこのような異議申立をしなかった。

しまった。「その結論は役立つというよりむしろ害を及ぼすのではないか」[89]。

④ Gorsuch 裁判官は、その反対意見において、次のように独自の考え方を展開した。発展中の技術の対処に当たって、裁判官の直感より実定法（positive law）のほうが頼りになり、詳細な手引きを提供できる。連邦通信法は、基地局位置情報を「顧客の独自のネットワーク情報」の一種とし、顧客に訪問権及び一定の使用コントロール権を与えている[90]。顧客の同意がなければ、携帯電話会社による通信サービスの提供の目的以外に使用、開示などできない[91]。第三者への開示も顧客の明確な委任状の提示が必要とされる[92]。携帯会社が義務違反した場合、顧客は損害賠償を求める民事訴訟を提起できる[93]。したがって、現行法の下で個人の基地局位置情報は修正四条にいう当該個人の書類又は所持品に相当するものといえる。ところが、Carpenter がこの点を見逃し、プライバシーの合理的期待ばかりを強調し、実定法上の権益の主張をあまりしなかった。そのため、彼の訴えを認めない[94]。

---

(89) 138 S.Ct.2206, 2247-2261 (2018).

(90) 47 U.S.C. § 222 (h) (1) (A).

(91) 47 U.S.C. § 222 (c) (1).

(92) 47 U.S.C. § 222 (c) (2).

(93) 47 U.S.C. § 207.

(94) 138 S.Ct.2206, 2261-2272 (2018).