経験から、政府の目的が恩恵を受けている場合は、自由を守るために最大限の注意を払う必要があります...  
–最高裁判所正義のルイ・ブランダイス正義の管理さえも、秘密はすべて退化しています。それがどのように議論と宣伝に耐えられるかを示さない安全なものはありません。  
– Nick Bohm、Ian Brown、Brian Gladman  
監視から監視、プライバシーから安全、市場競争から公正な選挙に至るまで、政府はオンラインでこれまで以上に関心を持っています。  
彼らは、テロや反乱、国家の戦略的および経済的優位性から、有害または不人気なコンテンツの抑制および人権の維持に至るまで、多くの具体的な政策的懸念を具体化しています。  
インターネットは、電気、蒸気エンジン、執筆、農業、そして火といった、他の大きなテクノロジーのように、多くの複雑な方法で世界を変えてきました。  
初期の頃、PCがメインフレームに取って代わり、インターネットがすべて開放されたため、多くの開拓者がユートピアでした。私たちは、情報への無料アクセスが個人レベルで解放され、権威主義政府も不安定化すると信じていました。  
2001年9月11日のニューヨークとワシントンへのテロ攻撃は、大規模な監視に対するインセンティブを生み出し、それに対する政治的反対を弱めることによって、本当の影響を与えました。  
振り子が2010年代に監視資本主義に向けて振り返った一方で、COVID-19のパンデミックは、プライバシーとセキュリティではなくプライバシーと健康のトレードオフで、国家監視をもう一度増やすように見えます。  
これは、2013年にEd Snowdenによって明らかにされたNSA機能だけではありません。ロシアや中国のような国家国家の競争相手も真剣な能力を持っています。一方、シリアのような発展途上国では、より原始的でありながら効果的なシステムがあります。  
米国とイスラエルはStuxnetマルウェアを使用して、イランの核兵器取得の攻撃に損害を与え、遅延させました。これにより、他の州がさまざまな種類のサイバー兵器を取得することを急いでいます。  
多くの厄介な問題があります。  
 もしそうなら、それについて私たちは何ができますか？  
9/11以降、通信の大規模な監視から裁判なしの拘留や拷問に至るまで、次々と権威主義的な措置が見られます。  
自由を守るより良い方法を見つけられませんか？  
 第二に、安全保障の政治経済があります。  
誤った場所に置かれた力の悲惨な上昇の可能性が存在し、持続します。  
左派と右派の政治家たちは、セキュリティ機関と報道機関に悪用され、恐怖の文化を煽っています。  
セキュリティ技術の議論は、立法者を脅かしたり脅したりするためによく使用されます。  
しかし、9/11以降、これはすぐに28日間に引き上げられました。その後、政府は、容疑者から押収されたPC上のデータを解読するのが困難である可能性があると主張して、90日を必要とすると述べました。  
警察が「容疑者を90日間拘束する必要があるのは、ソマリ語の通訳が足りないためだ」と言ったばかりの場合は、常識が入り込んでいた可能性があります。議会は彼らに商業翻訳代理店のスタッフを使うように言ったのかもしれません。  
暗号法を理解している人は、話す義務があります。  
現在、犯罪全体の約半分がオンラインになっていますが、それを解決するために費やされているリソースはごくわずかです。  
検閲に関してはさらに問題があります。  
虐待は、最上位での殺人や児童強姦の動画から、悪意のある表現、強姦の脅迫、サイバーいじめ、大規模な場合には有毒である可能性のあるニュースの操作まで、深刻なものまでさまざまです。  
企業は追加費用を嫌い、思慮深い市民は検閲が私的独占の手中にあるという考え、または写真やビデオから私的なメッセージまで、私たちがアップロードするすべてのものがフィルタリングされるという考えを嫌います。  
このような議論は、2019年3月にニュージーランドのクライストチャーチにある2つのモスクで射手が人々を殺し、Facebookを使用して犯罪のライブビデオを共有した場合など、重大な事件では氷を切りませんでした。  
COVID-19のパンデミックにより、会社はこれまで業界が不可能、望ましくない、または非現実的であると非難していた多くのことを迅速に行うようになりました：誤った情報の削除、搾取的な広告の禁止、公式の助言のプッシュ[984]。プライバシー規制はすでに複雑です。  
法律は細分化されており、健康データやビデオレンタルなどの特定のトピックに関する連邦法や、公開されたプライバシーポリシーに違反するFTCの罰則のある会社があり、州の法律はセキュリティ違反の開示を推進しています。  
全体として、IT業界の観点から見ると、ヨーロッパは世界のプライバシー規制者になりつつあります。ワシントンは気にせず、他の誰も気にするほど大きくはありません。  
 この章では、監視の進化について説明し、次にテロリズムを調べてから、検閲とプライバシー規制について説明し、最後に全体を文脈に入れようとします。  
26.2監視  
2つはさまざまな方法で相互作用します。  
中国のような他の国では、これらの企業は当局への完全なアクセスを与えることを拒否したため禁止されています。イランやシリアなどの他の国では、警察機関が人々のパスワードを暴行したり、友人をフィッシングしたり、電話をハッキングしたりしています。  
  
定規は常に通信を制御しようとしました。  
近世初期の州の開封およびコード解読施設、いわゆるブラックチャンバーは、デビッドカーンの歴史 『コードブレイカーズ』 [1001]に記載されています。  
ほとんどのヨーロッパでは、電信サービスは郵便局の一部として設置され、政府が所有していました。英国では、電信業界は1869年にグラッドストーンによって国有化されました。  
 物事を標準化するために1865年に設立されました[1818]。  
北軍と南軍の兵士はお互いの電信回線を盗聴し、ニューヨーク警察は1895年に盗聴活動を開始しました。  
米国では、最高裁判所は1928年にオルムステッド対米国で、住居の物理的な違反はなかったため、盗聴は捜査と押収に関する4番目の改正条項に違反しなかったと判決しました。ブランダイス正義は有名に反対した。  
翌年、連邦議会は連邦の盗聴を合法化しました（Omnibus Crime Control and Safe Streets Actの「title III」）  
1978年、ニクソン政権の人権侵害に対する調査の後、連邦議会は連邦情報監視法（FISA）を可決しました  
1986年、電子通信保護法（ECPA）  
1990年代初頭までに、規制緩和されたサービスの携帯電話から自動転送への拡散が、モデムの適応エコーキャンセレーションなどの技術開発と同様に、盗聴する当局の能力を弱体化させ始めました。  
 FBIが承認した方法ですべての通信会社にネットワークをタップ可能にすることを要求しました。  
さらに1,598件の命令が全体的または部分的に外国諜報監視裁判所（FISC）によって付与されました  
9/11より前でも、一部のアナリストは、許可された盗聴と同じ数の不正な盗聴があったと信じていました[558]。  
第2に、諜報機関の裁定取引があります。NSAが正当な理由なしにアメリカ市民を盗聴したい場合、彼らは同盟国にそれを行い、後で有利に戻すことができます。  
そのような慣行は何年もの間当局によって拒否されましたが、スノーデンの漏洩はそれらが現実であることを示しました。たとえば、2.1で説明したように、NSAはGCHQを取得して、Googleデータセンター間のリンクをタップしました。  
。  
最後に、多くの国では、警察は令状ではなく召喚状によって電子メールやその他の保存された通信を入手しています。  
しかし、公式の図を2倍または3倍にする必要がある場合でも、民主主義政権は権威主義的なものよりもはるかに少ない盗聴を使用します。  
頻繁な通りの検問所から、少数家族の家のビレットパーティのメンバーを介して、強制収容所での大量投獄まで、侵入的な物理的対策もあります[1110]。  
たとえば米国では、約半分の州でのみ使用されており、20世紀のほとんどのタップは、ニューヨーク、ニュージャージー、フロリダの「マフィア」州で行われていました（ネバダ州とカリフォルニア州は現在追いついています）。  
ヨーロッパでも同様のバリエーションがあります。  
 2510〜2521、FISAの外国情報収集に関する規制は現在、50 USC 1801〜1811として米国の法律で規定されています。  
オランダの殺人捜査では、被害者のアドレス帳の全員を1週間タップして、死に対する彼らの反応を監視するのが一般的です。英国では、国内の盗聴には大臣令状が必要とされており、証拠として使用することはできません。そのため、警察は部屋のバグやコンピュータの悪用を代わりに使用しています。  
国際電話は何十年にもわたって日常的に記録され、興味があることが判明した場合に備えて数日から数週間保管されます。これは、他の多くの国で採用されているモデルです。たとえば、2008年のムンバイ大虐殺の後、インドはテロリストがパキスタンのコントローラーにかけた電話の録音を掘り出すことができました。  
CALEAが導入される前の1993年、米国の警察機関は盗聴に5170万ドルしか費やしませんでした。おそらく、問題が政治化する前の価値の適切な見積もりです[862]。  
VoIPの方が難しい：「VoIPインターセプトの困難さのパラダイムは、絶えず場所を変え、たとえばボストンのカフェからパリのホテルの部屋に、そしてケンブリッジのオフィスから1時間後に電話をかける2人の出張者の間の電話です。ルーブルのギフトショップへ」[220]。  
したがって、政策立案者の傾向は、アクセスの限界コストを削減する設備投資を行うことです。  
現在、数億ドルを費やしていくつかの法律を通過させた後、彼らは携帯電話の場所のデータベースにアクセスでき、必要なのはデータベースクエリだけです。  
米国はまた、大量監視を容易にするために法律を変更しました。  
、所有者の知らないうちに家や企業を「こっそり覗いて」検索し、金融、電子メール、電話の記録にアクセスするためのFBIによる国家安全保障レターの使用。  
2005年12月、ニューヨークタイムズ紙は、ブッシュ大統領が、法律に反して、テロリズムの疑いのある米国住民の無許可の盗聴を強制する2002年の秘密命令に署名したことを明らかにしました[1606]。  
 AT＆T、Verizon、BellSouthの2億人の顧客にとって、米国の3大電話会社です。  
Qwestは協力しませんでした。当時のCEOであるJoe Nacchioは、NSAには裁判所命令が必要であると主張していました。  
彼らは、裁判所は彼らに同意しないかもしれないと言って、拒否しました。  
2007年10月、ベライゾンは上院議員に、2005年以来720回、国家安全保障書簡に対してFBIの第2世代の電話データを顧客に提供したことを認めた[1376]。  
2年間の議論の後、議会はFISAを改正し、不法な盗聴に協力した電話会社に遡及的な免責を認め、法律を変更し、NSAがFSAの令状を必要とせず、一方の当事者が米国または米国外の人。  
   
歴史的に、より多くの警察通信インテリジェンスは、盗聴ではなく、通話データの記録やその他のメタデータの分析に由来しています。  
繰り返しますが、これは新しいことではありません。  
1840年に郵便切手が導入されたことで、匿名で手紙を送ることがはるかに容易になったため、プライバシーの進歩が見られました。  
一方、電信の開発は監視の進歩でした。メッセージは送信者、受信者、単語数ごとに記録されるため、トラフィックの合計をまとめることができ、経済活動の効果的な指標であることがわかりました[1818]。  
後に20世紀の紛争がこれを補強した。  
 ペンレジスター（ターゲット電話回線からダイヤルされたすべての番号を記録するデバイス）  
 トラップアンドトレースデバイスの場合（発信者がブロックしようとした場合でも、着信コールの発信回線IDを記録します）  
法執行機関も1990年代に電話会社のデータベースの通話詳細記録に召喚状を使用するように切り替え始めていました。  
7つのベイビーベル全体に拡大すると、1990年代に毎年50万人の顧客が記録を押収されていたことが示唆され、トラフィックデータが盗聴された人のおそらく100倍の人数で収集されたことがわかります。  
Snowdenが2013年に世界中のすべての通信用のかなりすべてのトラフィックデータのデータベースを構築したことを明らかにした後、議会は2015年に自由法を可決し、National Intelligenceの局長から年次統計透明性レポートを取得し始めました。  
盗聴令状は、米国で年間約1,500で安定しています（約300人の米国人と1000人を対象としています）。さらに、通信コンテンツが取得された7,512人の米国居住者がいました（例：  
 一方、16,924人の居住者にはコンテンツがありませんでした（交通データなど）  
また、87,834の収集されたビジネスレコードがあり、これには、どの加入者がどのIPアドレスを使用しているかのレコードが含まれる場合があります[1464]。  
。  
誰かがテロ攻撃で爆破した場合、アナリストは、彼らが通信したすべての人々、次にこれらの直接の連絡先全員を監視するソフトウェアを使用します。  
これらの連絡先は、さまざまな容疑者リスト（宗教的過激派、右翼憎悪グループ、組織犯罪）の数百万人の名前と比較され、アナリストは既知の容疑者とのつながりを理解します。  
 したがって、アナリストは死んだテロリストや一部の宗教グループのメンバーと接触したわずか6ダースの人々を見るかもしれませんが、何万人もの無実の人々がソフトウェアによってコールデータレコードを見られました。  
 この方法で自動的に調査されました-2016年の151,230,968からの大幅な増加。  
 失効する。  
通信データの大量収集は、最も論争を巻き起こしたEd Snowdenによって強調された問題の1つでした。  
。  
別の資料を読むと、Boundless Informantは米国の通信プロバイダーを通じて30億の電話記録を収集し、さらに世界中で970億の電子メールと1,240億の電話を収集しました[816、p。  
98]。  
2020年に、この条項は3月に失効することが許可されましたが、5月に復活しました。政治は乱雑だった。  
いずれにしても、行動は普通の電話システムからメッセージングシステムに移行しています。  
これは、犯罪である可能性があります-重罪またはその他の犯罪-および連邦法または州法のいずれか。  
米国司法省は、国家安全保障のない法執行活動の統計を発表することを法律で義務付けられていますが、そうすることには消極的です。アメリカ市民自由連合（ACLU）  
 訴訟では、電話をスパイするために使用されるペンレジスタとトラップおよびトレースデバイスの元の注文の合計数が、2009年の23,535から2011年の37,616に60％増加したことが明らかになりました[765]。  
交通データへの大量アクセスもヨーロッパで深刻な政治的闘争につながっています。  
指令は、デジタル著作権アイルランドが包括的なデータ収集がEUの基本的権利憲章に違反していると主張する訴訟を起こした後、2014年に欧州司法裁判所によって打倒されました。  
データ保持指令に従い、ブレア政府は物事を集中化したいと考えました。警察は「通信データベース」が必要だと主張し、それを確立するために法律を推進した。  
多くの大臣や他の大臣が恥ずかしい主張をしていたことが判明した。数人の名誉あるメンバーが刑務所に行き、イギリスの有名な政治家のほとんどは返済しなければなりませんでした。  
 議会の承認がなくても、とにかく構築しただけだと2013年にEd Snowdenに言われるまで、通信データベースについては何も聞いていません。  
欧州裁判所が最終的に異議を唱えることは明らかでしたが、いくらかのスペースが必要であり、法律によりこれが与えられました（2年間の日没条項があり、キャメロン首相の自由連立パートナーはこれ以上彼に与えません）  
最終的に、英国離脱投票の結果として、議会は調査権力法を可決しました。これにより、GCHQは自由に行動できるようになり、管轄区域の会社にそれを支援するよう強制することができます。  
後でこれらの問題に戻ります。  
26.2.3検索語句と場所データ  
その当時、あなたは完全な盗聴をしてコンテンツを記録するか、通話データレコードからのトラフィックデータを処理しました。  
一部の人々は、URLをフェッチするページのアドレスと考えているかもしれませんが、http：//www.google.com/search？  
明らかに、一部の警官はそのような問い合わせを提出したすべての人のリストを望んでいます。  
米国では、司法省は、2か月分の検索クエリとインデックス内のすべてのURLを引き渡すために、複数の検索エンジンに召喚状を発行し、その主張を強化するためにデータが必要であると主張しました。児童オンライン保護法は憲法に違反しておらず、そのフィルタリングは児童ポルノに対して効果的である可能性があります。AOL、マイクロソフト、ヤフーは静かに対応しましたが、グーグルは反対しました。  
次の問題は携帯電話の位置データであり、異なる管轄区域では異なる扱いを受けていました。  
 2英国がEUから離脱すると、EU機関である欧州司法裁判所から逃れることができますが、これは人権裁判所ではなく、欧州評議会がプライバシーを侵害するためです[1926]。  
しかし、これらの規則にもかかわらず、情報の大量の漏洩がありました。  
位置データは現在、COVID-19の被害者の接触と疫学をより一般的に追跡する目的で、多くの政府によって収集されています。  
  
通話データの分析は、はるかに広い問題の1つの側面にすぎません：バルクデータセットの法執行機関による照合。  
調査官は、ユーティリティの使用に不規則なピークがあり、家賃と電気代が一連の異なる場所からのリモートクレジット転送によって支払われた賃貸アパートを探しました。  
この種の分析を行うためのツールには、交​​通分析や主要な警察捜査の管理に使用される多数の製品が同梱されています。  
また、商用および政府のデータプロセッサで使用される多くの独自のデータ形式を理解するコストによって課される実際的な制限もあります。  
AlphaGoは2016年にリーセドルを倒して以来、多くの機械学習の新興企業が存在し、法執行機関を何らかの方法でより簡単にすることを目的としたものは数多くあります。  
テロリストは、人口の割合として非常にまれであるため、偽陽性に溺れないようにするために、それらを「検出」するために使用するテストでは、非常に特異性が必要になります。  
IBMのデータマイニング業務のチーフサイエンティストであったジェフジョナスは、次のように述べています。「人々の行動を調べてテロリストの意図を予測する手法は、私が彼らを何もないと見なすのに必要な正確さのレベルに達するにはほど遠いしかし、市民の自由の侵害エンジン」[757]。  
26.2.5 ISPおよびCSP  
 および通信サービスプロバイダー（CSP – GoogleやYahooなどの企業）  
ISPでのデータトラフィックの盗聴は、以前の音声よりも困難です。ほとんどの顧客に与えられる一時的なIPアドレスや、ますます分散するトラフィックの性質など、多くの障害があります。  
、ISPにはモデムラックと、盗聴装置を配置できるLANがあった可能性があります。現在、多くの顧客がDSLを介してアクセスしており、プロバイダーは、タップするための明確な場所がないことが多いスイッチドネットワークを使用しています。  
現在、多くの国でISPに支援を求める法律があり、大規模ISPでこれを行う通常の方法は、対象のパケット（またはNetFlowレコード）のコピーを送信する機器をすでにインストールしていることです。  
FBIのシステムであるDCSNetは非常に洗練されており、エージェントはポイントアンドクリックで、参加している電話会社からのトラフィックやコンテンツにアクセスできます[1761]。  
 そして、警察はISPを理解していないため、事態はしばしば失敗します。間違ったものを召喚したり、不正確なタイムスタンプを提供して、間違ったユーザーをIPアドレスに関連付けたりします。  
スマートフォン革命により、自然な制御ポイントがISPからCSPに変わりました。  
これらの場合のいずれにおいても、ISPでの盗聴は、特定のサービスが使用されたという事実をはるかに超えて何も伝えません。  
これがFBIがPrismシステムをセットアップするきっかけとなりました。これにより、諜報機関はボタンを押すだけでGoogle、Yahoo、Apple、Microsoft、Facebookなどから顧客データを取得できます。  
このような法律を通過させる国が増えており、サービスプロバイダーは他の国の法律と矛盾します。  
しかし、もっとたくさんあります。  
そして、Googleの上級幹部が私に言ったように、「インドの家庭裁判所がカナダに住んでいて生涯の秘密保持命令を課する誰かのGmailを引き渡すように命じた場合、どのように同時にインドで人々を雇用し、信頼できる保証を与えるのですか？カナダの人々へのプライバシー？  
セクション11.2.5で説明したように、Michal Kosinskiと同僚は、4人のFacebookのいいね[1086]から、誰かがストレートかゲイかを判断できると考えました。キャンペーンの結果、2016年にソーシャルネットワークデータが英国のBrexit国民投票と米国の大統領選挙の両方に違法かつ大規模に介入するために使用されたことが発見されたときに、Cambridge Analyticaスキャンダルにつながりました。（これらの手法によって提起されたより広範な問題については後で説明します。）  
26.2.6ファイブアイズのシステム体系  
これらは完全に青から来たのではありません。シグナルインテリジェンスコレクションについては、以前に多くの開示がありました。  
後にPerry Fellwockと呼ばれた匿名の元NSAアナリストは、1972年にNSAの運用規模を明らかにしました[674]。  
「それは、外国政府が何をしているか、計画しているか、過去に何をしたかをカバーしています：どの軍がどこに、誰に対して反対しているか。どの空軍がどこに移動しているか、そしてそれらの能力は何か。  
その使命は、ベトナムのB-52での召喚から、ソビエト宇宙計画のあらゆる側面の監視に至るまで、あらゆるところに及んでいます。」フェルウォックの動機はベトナムに反対だったが、次の主要な内部告発者はイギリスの戦時中のコードブレーカーであるフレデリックウィンターボサムであり、彼は戦時中の業績の回想録を書きたかったが、死にかけていたため、起訴に悩まされなかった。  
 [438、1002、2007]。  
内部告発者のペグニュースハムは、NSAが上院議員のストロムサーモンドによる電話を不法にタップしたことを明らかにしました[373、374]。  
米国の経済スパイ活動に関する最初の注目度の高い発表は、1999年の欧州議会への報告[644]で行われ、ソ連崩壊後、EU加盟国がNSAの主要なターゲットになることを懸念していた[644]。 377]。  
、敵国を越えてトラフィックを収集する商用通信衛星および特別なSigint衛星との間のトラフィックの観測を通じて、加盟国の大使館のリスニングポスト[644]。  
電子戦を実施する能力がなければ、近代国家は空中戦、海戦、さらには戦車戦でさえ競争力がない。  
潜在的な敵のシグナルを理解するために、依然として多くの努力が費やされています。  
政治家はテロに関して9/11以来その予算を正当化しており、実際にテロリストに対していくつかの成功がありました-特に彼が既知のテロリストによって購入されたバッチから携帯電話のSIMを使用した後の主張された9/11テロ計画の逮捕スイスの。  
そして、人間の知性にもっと力を入れるべきだったことは明らかです。  
キリストのために、ほとんどの事件担当官はバージニア州の郊外に住んでいます。  
アフガニスタン、イラク、シリア、北アフリカでの戦争が始まってから20年近くが経過しましたが、アラビア語、ダリ語、プシュトゥ語で基本的な会話を行うだけの兵士を訓練していません。  
他の国でも諜報活動を行っており、経済やその他の非軍事スパイ活動を実施することで、はるかに攻撃的であることがよくあります。  
確かに、他の場所と同様にSigintにはネットワークの影響があります。インドのような非同盟国は旧ソ連から軍用機を喜んで購入しましたが、現在、米国よりもはるかに大きいネットワークを持っているため、米国と情報を共有する傾向がありますロシア人または中国人[84]。  
私自身の見解では、軍が所属することが多い軍のように、信号諜報機関は両方とも必要であるが潜在的に危険であるということです。  
問題は、そのようなリソースが存在するかどうかではなく、どのように説明責任を負うかです。  
スノーデンの啓示は、効果は限定的ではあるものの、米国政府の3つの武器すべてによる行動につながりました3。  
NSAは3人の大統領オバマがNSAレビューグループを立ち上げ、その勧告のほとんどを受け入れたが、彼の前向きな仕事はトランプ大統領によって取り消された。  
ロバーツ裁判長はFISA裁判所にいくつかの変更を加えました。  
あなたがNSAのディレクターであり、エンジニアの1人がWindowsのクールな新しいゼロデイエクスプロイトを利用しているとします。  
 それらの言葉で述べれば、答えは明白です。  
グループは、ほとんどすべてのケースで、NSAの注意を引く脆弱性を修正のためにベンダーに報告することを推奨しました。 NSAは代わりにそれらを備蓄することを好みます。  
そして、バグが自然に発生すると、NSAはバグを可能な限り使用します。たとえば、2014年に報告されたように、SSLの非常に破壊的なHeartbleedバグがNSAによって2年間悪用されてから、独立して発見および修正されました[2065]。しかし、ほとんどの国では、インテリジェンスの監視については議論さえされていません。  
新しいケースでは、電子的方法と人間の方法の両方による過剰な収集が継続的に強調されています。  
これは、過去数十年にわたって監視がどのように進化してきたかを示す高レベルの図です。  
国境を越えた帯域幅は、Ed Snowdenによって記述されたシステムが構築されていた2007年の11Tビット/秒から、2017年には704Tビット/秒に増加しました。このフレアホースは、ISPやバックボーンからではなく、CSPや他のエッジシステムからトラフィックを収集するように機関にさらに圧力をかけます。  
 監視と技術政策の問題について。  
26.2.7暗号戦争  
私は研究と教育が提案された統制の脅威にさらされている学者の1人として関わっていました。1998年に私は英国のインターネット政策シンクタンクである情報政策研究財団を設立し、これに取り組みました。暗号化ポリシー、エクスポートポリシー、著作権、および関連する問題。  
 他のヨーロッパのNGOとともに、ブリュッセルでこれらの問題についてキャンペーンを展開しました。  
  
19世紀半ばに多くの国が電信メッセージでの暗号の使用を禁止する法律を制定し、承認されたリストにある言語以外の言語の使用を禁止する国さえありました。  
時々、言い訳は法執行であり、人々が「公式」のトランスミッションに先立って競馬の結果や株価を入手するのを妨げましたが、本当の懸念は国家安全保障でした。  
連合国が第二次世界大戦中に信号インテリジェンスを使用して計り知れない成功を収めた後、イギリスとアメリカの政府は1946年に情報協力を継続することに合意しました。  
彼らは、暗号化機器とノウハウの急増を防ぐことにしました。  
これは、「輸出許可などを希望する人への最低限のオープンなガイダンスで、可能な限り秘密の方法で実施された輸出管理によって強化されました。  
 トラフィックへのアクセスを与えるでしょう。  
彼らが大企業だった場合、政府との契約が失われる恐れがあります。小さなものの場合は、ライセンスや製品の承認を得ようとするときに、赤いテープで首を絞められる可能性があります。  
しかし、ボウラーのケースで学んだように、これはすべての話ではありませんでした。  
彼は1992年にイランで逮捕された。当局がイラク人がイラン-イラク戦争中に彼らの交通を読んでいたと指摘したとき。彼らは、NSAが平文を手に入れることができるように改ざんされた暗号マシンを彼らに売ったと彼を非難した。  
その後、バウラーはスイスのラジオとテレビで、会社はドイツの諜報機関によって密かに管理されていて、長年にわたって諜報活動に関与していたと主張した[335]。  
Hagelinは彼の会社を密かにNSAに売却し、NSAはドイツの候補者によって密かに管理されていました。  
Crypto AGの主張は、これらの主張はNSAが企業を弱体化させるためにNSAによって作成されたというものでした。  
現在、Crypto AGは、ドイツのBundesnachrichtendienstがデンマーク、スウェーデン、オランダ、フランスの機関、およびCIAと共同で運営していたことが知られています。  
  
初期の銀行の暗号システムの質が低いにもかかわらず、NSAは70年代、依然として銀行セクターが自然界に逃れる優れたアルゴリズムを進化させるのではないかと心配していました。  
銀行業界が立派な暗号を欲しがっているのは、米国だけでなく海外でも、この暗号が外国政府に採用されたり、情報収集のコストを押し上げたりすることなく、どうすれば失われるのでしょうか。  
。  
これは意図的なものであることがわかりました。  
しかし、そうした印象を与えることにより、彼らはほとんどの外国政府がそれを採用するのを止めることができた。  
このような暗号で重要なデータを暗号化した外国人は、そのトラフィックを収集する価値があるとマークしただけです。  
1970年代には、これは関係者への嫌がらせによって直接行われました。 1980年代までには、より微妙な戦略へと進化しました。  
’DESに「トラップドア」が挿入されている可能性があるというほのめかしは、このプレイブックによく合いました。  
1990年代半ばまでに、このラインは使い果たされました。クリッパーチップの発売により、暗号化政策は1993年に主流になりました。  
これは、改ざん防止チップに実装された、分類されたブロック暗号であるSkipjackを使用し、スペア（「エスクロー」）を作成するプロトコルを使用します。  
この「エスクロー暗号化標準」は、公の抗議を引き起こしました。 AT＆Tコンピュータサイエンティストのマットブレイズは、エスクローメカニズムを無効にするクリッパーにプロトコルの脆弱性を発見し[258]、提案は取り下げられました。  
キーエスクローは、キーリカバリなどのさまざまな新しい名前を取得しました。クライアントの秘密の復号化キーのコピーを保持する認証局は、Trusted Third Parties（TTP）として知られるようになりました  
英国では、主要なエスクロープロトコルが公共部門に導入され[980]、これは民間部門にも採用させるために使用されました。しかし、そこにもいくつかの脆弱性が見つかりました[115]。  
反エスクローロビーは、暗号化はプライバシーに必要であるため、暗号を無効にする方法はあり得ないと主張することから始まりました。  
ほとんどの暗号化アプリケーションは機密性ではなく認証に関するものなので、それらを妨害するのではなく、警察を助けます。  
目立たないようにしたい場合は、プリペイド電話を購入することをお勧めします。  
最後に、警官にとってより深刻な問題は、許容できる証拠を見つけることです。これについては、まともな認証も役立ちます。  
米国のソフトウェア会社は、解読が困難な暗号を含む製品を輸出することを許可されておらず、これは家庭で暗号を制御する手段としても使用されていました。暗号化ソフトウェアをWebサイトに配置したアメリカ人は、外国人がそれを利用できるようにしたとして起訴される可能性がありました。  
彼の製品が市場のリーダーシップを獲得したため、彼はフォークヒーローになり、大金を稼ぎました。  
紛争は国際的になりました。米国国務省は他の国にも暗号を制御するように説得しようとしました（以下の輸出管理に関するセクション26.2.9で詳しく説明します）  
アメリカの政策を世界中に課すことは、ゴア副大統領の使命の1つになりました（2000年に多くの技術者がブッシュのキャンペーンに貢献した理由です）  
暗号化戦争1の明らかな解決策は2つのフェーズで行われました。  
これにより、NSAとGCHQから、すべての秘密署名鍵（復号鍵だけでなく、署名検証鍵も）をエスクローする必要があるという要求が損なわれました。  
EUがイギリスのラインではなくドイツのラインをたどったとき、個人は暗号化に署名キーペアを使用するか、Diffie-Hellmanキーを認証してそれらを暗号化に使用することができました。  
第2に、2000年にアルゴアが大統領に立候補し、シリコンバレーを倒したいと思ったときに、政府は停止を求めることにしました。  
代わりに、政府機関は多くの自然に発生する脆弱性を悪用し、NSAはパッチサイクルに侵入しました。  
これはNSAと共有し、修正のためにベンダーに報告します。  
ヨーロッパでデジタル著作権で活動していた私たちの人々は、一般に電子署名の指令に満足していましたが、無形の輸出規制にはぞっとしました。欧州デジタル権利（EDRi）を設立  
私たちは、監視の問題は大部分解決されており、将来の問題はソフトウェアの著作権やデータ保護などの問題をめぐる問題だと考えました。  
NSAと他の機関は単に地下に潜り込み、年間1億ドルの予算でBullrunと呼ばれる秘密のプログラムを実行して、商用暗号を弱体化させ、標準、実装、サプライチェーンなどに干渉していました。  
暗号戦争1のエンジニアリングの教訓の1つは、鍵のエスクローを適切に行うことが難しいことです。  
エスクローが必要な場合は、通常、シンプルなローカルメカニズムを使用するほうが適切です。  
こうすることで、キーは電子版で保護されているドキュメントと同じ場所に保管され、飛行機が爆撃したりスパイが盗んだりするための中央データベースはありません。  
英国政府のアイデアは、GCHQによって生成された超秘密マスターキーを使用して電子メールアドレスから全員の秘密鍵を生成し、部門のセキュリティ担当者が制御する機器に保管することで、部門とGCHQの両方がトラフィックを復号化できるようにすることでした。に。カスタマイズされた中央制御の需要により、膨大なITプロジェクトが数年遅れて実行され、予算を超えて実行されるか、まったく機能しない場合があります。  
 は、G Suiteの有料版であるG Suiteのブランドバージョンの使用を開始しました。  
暗号戦争1は、技術的側面と政治的側面の両方を備えた重要な遺産を残しました。  
ホテルのドアロックを販売する企業のビジネスモデルは、顧客が自社のカードストックを購入するためにロックすることができなくなったため、根本的に弱体化しています。  
 私が所有するキーまたはパスワードを私に渡すことを警察に要求することを可能にする2000年の法律、および2002年の輸出管理法は、56ビットより長いキーを使用する暗号化ソフトウェアをヨーロッパ国外に送信した場合に輸出許可を取得するように指示しています5 。  
  
エドワードスノーデンによる2013年の開示は、暗号戦争の流行後の再開につながっています。  
彼らはバックボーンから全員のSMSと電子メールを収集するだけでなく、私たちが想像したよりもはるかに大きな規模で令状を使用して主要なサービスプロバイダーからコンテンツを取得していました。  
別の例は、サモア、トンガ、フランス領ポリネシアなどの小さな隣人へのスパイ行為を含む、5つの目に対するニュージーランドの貢献でした[850]。  
彼らは法的規制を迂回していました。GCHQは私が米国の居住者ではないため、Prismを使用してGoogleからGmailを取得する可能性があり、私たちはこれを常に疑っていましたが、常に拒否されていました。  
4車の盗難についてはセクション4.3.1、Bluetoothへの攻撃についてはセクション5.7.2.2、セクション[？  
5ありがたいことに、エクスポートを行うのはリンクをクリックした人です。そのため、イランにいる場合、私のWebサイトのリンクをクリックして蛇のブロック暗号をダウンロードすると、非常に悪い人になります。  
これらすべてが行動に実際の影響を及ぼしました。  
MicrosoftとYahooが続いた。  
。  
 英国のような国々は米国のデータへのより迅速なアクセスを得るために尽力しましたが、他の国々はローカライズに行きました。  
たとえば、アフリカのほとんどの国では、財務データをローカルに保持する必要があります。欧州連合のデータ保護規制とそれと米国企業との相互作用については、後で説明します。  
GCHQはFBIとともに、WhatsAppやFaceTimeなどのメッセージングサービスのプロバイダーに、法執行機関を無言の電話会議当事者（いわゆる「ゴーストユーザー」）として追加できる施設を構築するよう強いられるべきだと主張し始めました。  
FBIのディレクターであるジェームズコミーはGCHQのディレクターであるロバートハニガンとともに率いる責任者を率いました。  
彼とコミーは英国首相デビッド・キャメロンによって支持されました。  
現在、1990年代よりもインターネットへの依存度がはるかに高いため、何らかの影響があれば悪化する可能性があります。  
例外的なアクセスを構築すると、盗聴システム自体に大きなターゲットが作成され、さらにセキュリティの障害につながる可能性のある複雑さが増します。  
中国人は明らかにアメリカの彼らのエージェントのどれが疑われていたか知りたいと思った。  
FacebookがフランスのユーザーからアルゼンチンのユーザーにWhatsAppメッセージを運ぶ場合、これら2つの政府だけがアクセスできますか、それともNSAもそれを要求しますか？  
このようなシステムに対する需要は、法律と工学の両方に多くの疑問を引き起こします。その一部は、分析で詳しく述べています[5]。  
AppleのTim Cookは以前バックドアをインストールするという圧力に抵抗し、このケースをAppleユーザーのプライバシーとAppleブランドに対する深刻な脅威であると見なしていました。彼は法廷でFBIと戦った[1006]。  
ケースはアメリカの意見を分け、共和党員はFBI（そして当時のトランプ候補はアップルのボイコットを求めていた）を支持した。  
私の同僚のSergei Skorobogatovは、3.4.8.3で説明したように、iPhone PINリトライカウンター[1777]を倒す方法を考え出しました。  
英国離脱国民投票に続く混乱の中で、新しい英国首相テレサ・メイ（家の秘書として監視のタカであった）  
この法律は、信号インテリジェンスの収集を容易にし、それについて永遠に静かに保つために、物理的に可能なことをすべての会社に命令する権限を大臣に付与します。私の同僚のBruce Schneierは詳細に回答しました[1678]：そのようなアプローチは一部のシステムでは機能する（WhatsAppでは機能するが、Signalでは機能しない）という事実  
いずれにしても、そのようなアクセス権は過剰です。諜報機関は、そのようなアクセスを悪用したり、単に失ったりした歴史があるため、それを持っているべきではありません。  
Mark Zuckerbergは2019年に、WhatsAppをInstagramとメッセンジャーと統合することにより、Facebookがその重要性をパブリックポストからエンフェメラルなエンドツーエンドの暗号化メッセージングに移行することを発表しました[1439]。  
10月、米国司法長官は英国内務大臣とオーストラリア内務大臣に加わり、Zuckにもう一度考えさせ、「アクセスできないメッセージングサービスとオープンプロファイルを組み合わせ、犯罪者候補に独自のルートを提供する単一のプラットフォームのリスクを強調しました。私たちの子供たちを特定して手入れするため。  
  
暗号化戦争からの波及の1つは、特にヨーロッパで、以前よりも均一な輸出規制が課されたことです。こちらが簡単な要約です。  
 暗号機器の輸出規制を実施するためにほとんどの政府を拘束し、後者はEU規制によりEU規制によって実施され、加盟国にデュアルユース商品（民間および軍事用途の両方を有する商品）の輸出を規制および認可するように強いています。  
国家政策は以前よりも多様でした、そして1990年代の間、私のようなヨーロッパの研究者は暗号ソフトウェアを作成して私たちのWebページに公開することができましたが、米国の同僚は米国の国際人身売買規制（ITAR ）  
米国企業は不満を表明し、1997年にアルゴア副大統領が次期英国首相のトニーブレアを説得し、無形資産への輸出管理を拡大しました。  
（そのような政策ロンダリングは、言われているように、ヨーロッパでは風土病であり、英国をEUから離脱させる運動を後押しした要因の1つです。）  
 56ビットより長いキーを持つ暗号を含む。  
 使用できますが、メカニズムを理解し、書類を提出する必要があります。  
たとえば、ハードウェアの改ざん防止研究では、電子ビームワークステーションを使用します。これは電子顕微鏡のようで、電子ではなくターゲットで金属イオンを発射するだけなので、トラックをカットして新しいものを追加することでチップを修正できます。  
昔は輸出許可を取得しなければならず、7年後には輸出許可をスキップして取得しなければなりませんでした。  
実際の結果は、何万人もの科学者が喜んで法律を破ったことであり、これにより彼らは当局からの圧力に対して脆弱になります。  
私がそのような問題に個人的に対処する方法は、そのようなすべてのソフトウェアとスクリプトが私のWebサイトにあることに非常に注意することです。これにより、パブリックドメインの免除を使用でき、実行するのはリンクをクリックする人であるという事実に依存していますエクスポート。  
いくつかのデジタル著作権NGOの人々は英国政府に働きかけ、輸出管理法を使用して、英国の企業が大量の監視機器をアサド政府に販売するのを防ぐように求めました。  
GCHQの女性はこの歯と爪を戦いました。販売はドバイの武器販売業者を経由して行われたので、ベンダーはどのように宛先を確認できるでしょうか。彼らはドイツの子会社から来たので、ドイツ人の問題でした。 Wassennaarは人権問題ではなく軍事問題のフォーラムでした。さらに、その大量監視はマーケティングにも使用されます。  
結局、ドイツのアンゲラメルケル首相は、監視装置をシリアに売却することを許可することを決定したこと、そして彼女がとった最も難しい決定の1つであったことを公に認めました。  
やがて、輸出管理問題はヨーロッパの機関に紹介され、静かに忘れられました。  
GCHQは、暗号学を研究している中国の学生に反対し、セキュリティサービスは、イギリスで博士号を取得したイラク人女性が、サダムフセインの申し立てられた研究プログラムの一部を大量破壊兵器に向けて行ったことを説明しました。  
ウイルス学の教授でケンブリッジの同僚であるトニーミンソンは、自然は人々よりも多くの厄介なことをすることができると主張し、エボラのようなものがナイル川を下ったときにハルツームに有能な公衆衛生の人々がいなかった場合、私たちはそれを後悔します。「アカデミックテクノロジー承認スキーム」を取得しました。英国に来る大学院生は、ビザを取得するために「ATASクリアランス」を取得する必要があります。  
26.3テロ  
流れは後退し始めていますが、それは政治家が私たちを怖がらせたいときに演じるカードであり、メディアはしばしば共演します。  
それでは、テロについて何と言えますか？  
テロは、マヤ族、インカ族、ウィリアム征服者など、長い間、対象集団の牛に使用されてきました。  
ガイフォークスは1605年にイギリスの国会議事堂を爆破しようとしました。彼の後継者であるアイルランド共和軍は、イギリスに対して多くのキャンペーンを展開しました。  
冷戦中、ロシアはIRAだけでなく、ドイツや他の多くのバーダーマインホフギャングを支持しました。西側は、アフガニスタンでロシア人と戦うジハード主義者を武装および支持した。  
この歴史からどんな一般的な教訓を引き出すことができますか？  
  
最大の朗報は、テロ暴力の傾向が着実に低下していることです[1350]。  
多くはソビエト連邦またはその同盟国によって冷戦の代理紛争として調達されたが、一握りではあったが（特にニカラグアのコントラとアフガニスタンのソビエトへの抵抗）  
冷戦の終結は動機とお金を取り除いた。  
 要点は、内戦の原因の一部は経済的であるということです。  
、または貪欲によって（一部の反乱は他のものより経済的に実行可能です）  
世界には多くの不満がありますが、反乱の発生率はそれが持続できるかどうかによってより決定されたことをデータは示しています。  
 したがって、IRAキャンペーンはソビエト圏とリビアから多大な支持を得た。スリランカでのタミル人の反乱は、アメリカとインドのタミル人からの資金によって支えられました。そして、アルカイダは湾岸諸国の裕福なドナーによって財政を支えられました。  
もちろん、それだけではありません。 ANC（およびアンゴラとモザンビーク）に対するソビエトのサポートの喪失  
  
心理学者、政治学者、メディアの研究者からは、あまり励みにならない発見があります。  
セクション3.2.5で影響ヒューリスティックについて述べました。人々が影響、つまり感情に依存している場合、確率の計算は無視される傾向があります。  
9/11の結果として亡くなったアメリカ人のほとんどは、probablyyではなく運転することを決定した後の自動車事故でそうなったと考えられます。それ以来年間500 [1677]。  
トムピシュチンスキ、シェルドンソロモン、ジェフグリーンバーグによるテロの心理学に関する研究では、人々が死の恐怖にどのように対処しているかに注目しました[1564]。  
最初に全員に性格調査票が渡され、半分は「あなた自身の死の思考があなたに呼び起こす感情を簡潔に説明してください」などの質問がされ、私たち全員が1日で死ぬことを思い出させました。  
さらなる実験は、死亡率-顕著性グループが単に卑劣になっただけではないことを示しました：彼らはまた、何らかの公的行為を行った市民により大きな報酬を与える準備ができていました。  
これは、サイバーテロが発生しなかった理由を説明するのに役立ちます。  
メディア分析はこれを確認します。カバレッジは死亡率と強く相関しており、追加の死体ごとに46％増加します[1026]。  
応答に宗教（1950年代以来の最高レベルの教会出席率）が含まれるのは当然でした  
、一部の人にとっては偏見もあります。  
不思議なことに、彼らが死ぬことを思い出したとき、保守派もリベラル派も、留学生が書いた反アメリカのエッセイをより二極化して捉えます。事件の保守派は、自由主義者が主張するよりも激しく学生の言論の自由の権利を擁護している[1564]。  
これは、チャーチルのラジオ放送からルーズベルトの野外チャットまで、最高の指導者が行うことです。  
他の政治家は、再選するために恐怖を利用する誘惑に屈しました。  
イスラム過激派は78.4％の確率でテロリストと名付けられましたが、右端の過激派は23.6％の確率でテロリストとして識別されました。  
おそらく最も最近の反応は、ニュージーランド首相のジャシンダアーダーンがクライストチャーチでの発砲に対応したものだったのでしょう。彼女はそれを即座にテロリズムと説明しただけでなく、射手に名前を付けることを拒否した。いずれの場合も、メディアは[1335]に従いました。  
   
政府がなぜ彼らのやり方で行動するのか、そしてその創設者の1人であるジェームズブキャナンが1986年にノーベル賞を受賞した理由を説明することに専念する学問的なテーマ全体-公共選択経済学-があります。  
帝国は、生み出す利益ではなく支配の範囲によってランク付けされるため、帝国を構築するのは当然のことです。  
彼らの決定を理解するには、方法論的な個人主義、つまり国の潜在的な利益や損失ではなく、個々の大統領、議員、将軍、警察署長、新聞編集者が直面するインセンティブの分析が必要です。  
しかし、これは政治的にはより困難です。  
 国益はどのように定義されるのでしょうか？  
前者では個別にユーティリティを最適化しようとしますが、後者では同じことを行いますが、外部性やその他の障害のために市場で達成できない目標を達成するために集団行動を使用します。  
世代間の交渉は困難です。政治家がお金を借りて今すぐ投票を購入し、法案をまだ投票できない次の世代に任せるのは簡単です。  
 簡単に言えば、制度は重要です。  
1960年代の公共財政の問題に対応して、公共選択経済学が登場しましたが、いくつかの明確な教訓があります。  
職員も利害関係のあるエージェントなので、行政構造もそうです。  
そのため、すべてのペットプロジェクトが汚れてしまい、政治的な美人コンテストは、元の形では200億ポンドかかるであろう壮大なプロジェクトである全国のIDカードによって勝利しました[1182]。  
確かに、USAF大佐カレンクウィアトコウスキーはイラク戦争の開始時に引退し、諜報機関の評価が政治的にどのように操作されたかを説明し、後に議会に出馬しました[1113]。  
特に関心のある機関は、昔ながらのマスコミであれ、その機能の一部を引き継いでいるソーシャルメディアであれ、メディアでなければなりません。  
メディア所有者の自己利益は、再選を希望する政治家、帝国を築きたい政府関係者、およびセキュリティ製品を販売したいベンダーの利益と相まります。  
ファーマンジェリングは政治家を第一面に導き、彼らが議題を管理するのを助けます。  
  
しかし、人々は時間とともに学びます。  
国民の最初の反応はザラザラした辞任でした。「ああ、まあ、こういうことが起こるのはわかっていた。そこにいたら運が悪かったが、人生は続いたのだ。」6そして、人々が学ぶように、政治エリートもそうだろう。  
ケネディ、ジョンソン、ニクソン、フォード大統領はテロを無視した。  
サイラス・ヴァンス国務長官は後に、米国の外交官を誘拐したイランの「学生」に不当な信用を与えるのではなく、危機を軽視すべきだったと認めた。  
ただし、このエラーから距離を置くと、彼の評価はすぐに回復しました。  
英国でも同様のことが起こり、マーガレットサッチャーがテロリストを一般犯罪者として扱った後、2度再選されました。  
成熟した有権者は、テロリストに立ち向かう政治家を好む6マスコミはこれに数日間続いた：それから恐怖の爆発があった。  
それらを再選挙キャンペーンの小道具として使用するのではなく。  
何年もの間、パンデミックはイギリスのリスクレジスタのトップにありましたが、テロ対策に費やすよりもはるかに少ないものを準備するために費やされました。その多くは効果的というよりも目立たないものでした。  
米国と英国の政府は、2000年代にアルカイダの細胞が核爆弾を盗み、それをニューヨークまたはロンドンで爆発させたと話し、拷問を正当化した。  
中国、シンガポール、台湾、韓国の政府とは異なり、テロのレトリックは、公衆衛生を犠牲にして安全保障局を膨らませ、アメリカ、ヨーロッパ、インド、アフリカの政府に2003年のSARSの教訓を無視する素質を与えました。  
26.4検閲  
私はまた、「過去数年間で検閲がはるかに大きな問題になっている」と述べました。  
国家の検閲と、サービス会社によるコンテンツのフィルタリングという2つの面があります。  
ジョンウィクリフが1380–1年に聖書を英語に翻訳したとき、彼が始めたロラード運動は農民の反乱とともに抑制されました。彼らは彼を危険にさらしたが、それまでに新約聖書の50,000部以上が印刷され、宗教改革が進行中であった。  
最近の検閲はさまざまな動機で行われています。  
やがて、2004年のサイバー犯罪条約は、署名国に18歳未満の性的画像の禁止を義務付けました。  
英国は、テロを美化することによって若者を「急進化」させるウェブサイトを禁止します。  
インターネットの発明により、検閲者の仕事はある意味でより簡単になり、ある場合には困難になりました。  
ライブラリの物理的なコピーと少数の企業のサーバー（Amazonの電子書籍システムから主要な報道機関のサーバーまで）に人間の知識を集中化した場合、歴史的な記録を変更することは不可能でした。ある意味では、15世紀にさかのぼります。  
一方、今日では誰もが出版社になることができます。オンラインで本当に不愉快なコンテンツの多くは、ソーシャルメディア、新聞のコメントページ、嫌がらせや脅迫したい個人に、匿名で投稿した何百万人もの個人からのものです。  
10年前、中国には反体制派の発言を取り下げた何万人もの人々がいましたが、今では、何百万人もの市民ボランティアがそれを無視しています。  
問題を解決するために、いくつかの状況を見てみましょう。  
26.4.1権威主義体制による検閲  
しかし、当局は、あらゆる形の組織と党の支配外の人間の連帯を抑圧することにおいて着実に効果的になっています。  
その当時、中国には大都市の人口の4分の1を含む1億3700万人のインターネットユーザーがおり、「中国の大ファイアウォール」は、ポルノから宗教的な素材まで、さまざまな素材に対して徹底的な防御を提供する複雑な制御システムでした。政治的異議[1469]。  
まず、境界防御があります。  
TCPレベルでの詳細なパケット検査は、「法輪功」などの禁止された単語を含む電子メールおよびWebページを識別するために使用されます。このような接続は破棄されます。  
現在、ほとんどのトラフィックは暗号化されているため、それほど簡単ではありません。  
 これにより、トラフィックが行くサブドメインを告げる検閲が停止します。これは7月の初めまでにトラフィックの30％以上に達しました[433]。  
現在、サービスプロバイダーが監視と検閲の両方で体制を支援する準備ができているかどうかに応じて、ブロックされているサービスとブロックされていないサービスがあります。  
現在、最も重要な国境は国ではなく企業の国境であるので、中国政府はその産業政策をその政治と一致させました。  
言語には1つの障壁がありますが、強力な技術的な障壁もあります。境界の防御は、中国の居住者が未承認のサービスを使用するために使用できるTorとVPNのブロックに焦点を当てています。  
10年前にはすでに3万人のオンライン警察がいた。現在、より多くの市民がこのプロセスに従事しており、すべての反対意見を阻止しようとするのではなく、戦略はそれを制圧することです。  
社会的信用システムは、そのような向社会的行動に対して人々に肯定的なポイントを与えますが、反社会的と見なされるものに対してはポイントを失う可能性があります。  
2014年以降、新疆ウイグル自治区の「再教育」システムは、西部の「テロとの戦い」と毛沢東主義の社会的統制の融合技術を開拓しており、入力には、容疑者が定期的に祈るか、電話にVPNがあるかが含まれます。  
議会はこの体制を「人道に対する罪」であるとして非難しました。数十社の請負業者が制裁リストに載せられています[359]。  
ロシアのインターネットはかなりオープンで、政府は主なソーシャルネットワークを引き継いでおり、敵を怒鳴りつけるためにトロールの軍隊を組織していますが、野党政治家のAlexei Navalnyは、何百万人もの視聴者がいる自分のYouTubeチャンネルを所有しており、検閲電報は、街頭抗議に会った。  
アラブの春もまた重要です。  
抗議行動はFacebookやその他のソーシャルメディアを利用して組織され、政府の没落につながり、近隣諸国にも波及しました。シリア政府はほとんど崩壊しましたが、数十万人を殺し、数百万人を追放した内戦で反撃しました。  
私が2020年に書いているように、民主主義への移行を管理してきたのはチュニジアだけです。  
世界の独裁者たちが引き受けた教訓は、権力を維持するためには、中国で使われている方法をよりよく研究するということです。  
 しかし、それらのインフラストラクチャは、VPNやTorを使用してかなり簡単に破られます。  
アラブの春はどの程度技術の機能でしたか。また、これは順調に進んでいるように見えましたが、2011年にFacebookやGoogleのような企業によって宣伝されただけの誇大宣伝でしたか。  
立ち上がった人口の一部、特にリビアとイエメンの人々はインターネットをほとんど利用していませんでした。一方、2007年のビルマでの反乱は、人口のわずか1％しかアクセスできなかったにもかかわらず、インターネットによって引き起こされました[1471]。  
  
ヘイトスピーチに関する民主主義の法律は大きく異なります。  
しかし、解釈は異なります。  
 何十年もの間ドイツでは犯罪でした。  
サービス会社が悪いものを落とすことのコストについて何を言っても、ドイツの例は彼らが必要なときにそれを行うことができることを示しています。  
斬首の動画だけでなく、借金を返済しなかった顧客をドラッグギャングが撃つなど、殺人のすべての動画を禁止することは良いことのように思えるかもしれません。  
このようなポリシーを適用するプラットフォームは、現地での殺害と海外での人権侵害の両方の証拠を削除することになります。  
Facebookの元CISO Alex Stamosは、プライバシーと検閲の間の緊張をスペクトルとして説明しました：人々は、WhatsAppなどのエンドツーエンドの暗号化チャットが検閲されるのではなく非公開であり、放送メディアが非公開ではなく検閲されることを期待しています真ん中、Facebookグループのように。  
プラットフォームは大きく異なります。 Facebookはおそらく最もタイトで、ヌードさえ禁止している7。それは他のものよりトランプ大統領からのヘイトスピーチの方がはるかに寛容ですが、見返りに反トラスト法の面ではるかに少ない注意を受けているように見えます[1790]。  
禁止コンテンツを見つけようとするAIシステムの背後には、何千ものコンテンツモデレーターがいます。  
心地よさ[1438]。  
検閲を大規模なサービス独占企業に外部委託することも問題です。  
世界は、彼らが弱者を無視している間、金持ちと権力者による虐待を許すのを見ます。  
議論の焦点の1つは、1996年の米国通信品位法（CDA）のセクション230です。  
 一方、そうしなかった企業は、ディストリビューターとして扱われ、法的責任を免れることになります。  
 セクション230は、YouTubeやFacebookのような企業を可能にしましたが、ビジネスモデルがリベンジポルノ、名誉毀損、または違法な銃器の販売の削減に基づいているサイトを保護しました[1419]。  
当時、インターネットのユーザー数は1,000万〜2,000万人で、ほとんどがオタクでした。現在、ほとんどの人間の活動はオンラインで行われており、200を超える国々の検閲者、検察官、裁判官として行動するアメリカの企業の一部は持続可能ではありません。  
緊張はさらに悪化します。  
ティム・ウーの「注目商人」[2050]は、1830年代に最初の大衆市場新聞が登場し、恐ろしい犯罪報告や特許医薬品の広告を詰め込んだプロパガンダの歴史です。これは政治家に彼らの最初の産業大衆市場チャネルを与えました。  
次にテレビがあり、その性質は広告によって形作られました。人々は、クイズ番組や石鹸など、目玉をつかむために発明したものです。  
彼は政治的二極化の歴史をたどり、その結果の根本的な原因はテクノロジーやロシアの干渉ではなく、過去20年間に発展した左右の非対称メディアシステムではなかったと主張しています。左と中央の右は事実に基づいていますが、右は宣伝フィードバックループです[227]。  
偽のニュースに対する政府の反応はほとんど効果がありません。  
その政府は、2014年以来、学校などで批判的思考とメディアリテラシーを促進してきました。そのため、すべての市民の仕事は、部門をまくために設計された情報を見つけて対抗することです。  
教師や大学教授は、過激化のリスクがあると思われる生徒を報告し、セミナーやその他の講演で過激化する可能性があるかどうかを判断する手順を持っているはずです。それらを迷わせるかもしれないオンライン資料に対する法律もあります。英国のEU離脱キャンペーン中に英国議会の議員を殺害したことで、白人至上主義者は少なくとも同じくらい脅威です。しかし、私たちの政府はそれらを取り締まることにあまり熱心ではありません、そしてそのキャンペーンにあまりにも多くのお金（ロシアのお金を含む）を使うことによって法律を破った人々  
一般に、インターネットの検閲により、政府は何かをしていると主張することはできますが、実際にはうまく機能せず、外交官たちが言論の自由について世界中の専制君主に対して語る可能性のあることはすべて損なわれます。  
フィンランドが示しているように、長期的には、鍵は教育です。  
過激派組織にサインアップした数少ない英国の学生は、社会的に尊敬の欠如を経験し、おそらく仲間に拒否され、アイデンティティを探していましたが、両親の宗教にそれを見つけることができなかった学生でした–その後、他の不満の若者の小さなグループ。  
白人少年の白人至上主義者グループへの急進化は、大きな違いはありません。  
彼らのグループは、変化の主体ではなく、メンバーが離脱する制度になります。そのため、彼らは暴力を増して賢明な平和の申し出に対応し、同様のグループとの殺人紛争に従事することができます[6]。  
 テログループや犯罪集団に加わって身元を見つけることは、宗教、スポーツクラブ、ダンスバンドに加わって身元を見つけることと同じです[2022]。  
社会的連帯を求めて極端な組織に参加する人々は、自分を善人だと考える必要があります。あなたはそれを弱体化する必要があり、それらを除外することによってそれを行うことはできません。  
最良のアプローチは、人々を排除しない環境を用意することです。学生は、自宅の階段、小さな教育グループ、プロジェクトグループなど、さまざまな背景の人々と知り合い、何百ものスポーツと学生がいます。社会から選択するため、誰もが所属するギャングを見つけることができます。  
  
最後の主要なポリシングトピックは、証拠を使用するためにコンピューター、携帯電話、その他の電子機器から情報をどのように回復できるかです。  
コストの上昇と運用の困難さにより、より厳格な法執行が行われ、州が介入することの少ないオンラインの害のすべてのカテゴリが存在します。  
  
コンピュータフォレンジックは、少なくとも1980年代以降、警察にとって大きな問題となっています。 2000年代初頭までに、施設とスタッフのトレーニングの両方が絶望的に​​遅れをとっていました。  
警察が最近、短時間の麻薬の売人でさえ襲撃したとき、彼らは6ダースの携帯電話、いくつかのラップトップ、および彼の位置履歴を保持するナビゲーターやFitbitなどのガジェットを手に入れることができます。  
データから情報を抽出するためのあらゆる種類の巧妙な方法があります。たとえば、CCDアレイのパターンノイズから写真を撮ったカメラを特定し[1192]、これを使用して写真のどの部分を推測するかを決めることもできます。改ざんされています。  
捜査令状または同等の権限があるかどうかにかかわらず、資料は合法的に収集されなければなりません。また、法医学担当官は一連の監護権を維持する必要があります。これは、証拠が後で改ざんされなかったことを裁判所が満たすことができることを意味します。  
。  
世界がスマートフォンとクラウドサービスに移行して以来、重心は、警察および諜報機関にモバイルフォレンジックツールを販売する少数の企業にシフトしています。  
一部の警察は法的問題を整理するために懸命に取り組んでいます（警察スコットランドなど、令状なしに「クラウドフォレンジック」を使用していません）  
取引のより洗練された終わりには、法医学と対策の間の軍備競争があります。  
フィッシングギャングは、フィッシングソフトウェアをメモリに常駐させることでこれを悪用し、証拠が自動的に破壊されるようにしました。  
2013年までに、FBIがシルクロードの地下薬物市場の創設者であるロスウルブリヒトを逮捕したとき、エージェントの1つの使命は、ラップトップに手を入れてウルブリヒトが閉鎖するのを止めることであり、彼はそれを差し込むための適切な種類の電源コードをすでに持っていました[482]。  
現在、クラウドサービスのおかげで、人々は発作に強いオフサイトバックアップを利用できます。  
セクション26.2.8で言及したFacebookとGCHQの対立は、2013年3月にウーリッチの兵舎の近くで、2人のテロリストがイギリス人の兵士、リーリグビーを車で走らせて刺したことで殺害したときに発生しました。これには、ロンドンの米国大使館での警察の提出書類が含まれ、ワシントンの司法省で詳細に検討されます。  
すべてがうまくいったとしても、FBIがカリフォルニア州メンロパークのFacebookで書類を提出し、データを収集するのに6週間かかる場合があります。  
2017年頃から、3つ目の選択肢としてクラウドフォレンジックがあります。  
英国の警察の一部はこれを素晴らしいと考えています。ダウンロードしたデータは、携帯電話自体で検出された場合と同様に「保存データ」として扱い、永久に保持します。  
クラウドデータを取得するインセンティブは強力ですが、関連するメカニズム（電話のハッキングとそれに続くユーザーのなりすまし）  
そして、ますます多くのデバイスが、付属のクラウドサービスとアプリを取得しています。  
 これは2020年の現在の政策トピックです。たとえば、英国のプライバシー規制当局は法定の行動規範の開発を求めています[958]。  
  
1960年代に裁判所が最初にコンピューターの証拠に直面したとき、その信頼性について多くの懸念がありました。  
立法府がこれに異なる方法で取り組みました。  
 定期的に行われるビジネス活動の過程で保管されている場合、コンピュータデータを「知識のある人が送信した情報から、または送信された情報から、その時間またはその近くに作成したレコードとして導入することを許可します...  
 スティーブンメイソン[1236]によって分析されます。  
英国では、裁判所はメールが手紙と同じように書かれているとの見方をしました。署名の本質は署名者の意図です[2042、2043]。  
2000年、議会はグローバルおよびナショナルコマースにおける電子署名（「ESIGN」）を制定しました  
したがって、電話のキーパッドを押す（「0を押して同意するか、9を押してこのトランザクションを終了する」）  
これにより、アメリカではクリックラップライセンスが完全に有効になります。  
ヨーロッパでは、2000年に施行された電子署名指令が高度な電子署名に特別な影響を与えました。これは基本的に、スマートカードまたはハードウェアセキュリティモジュールで生成されたデジタル署名を意味します。  
多くの国では、紙の小切手が偽造されるリスクは証明書利用者が負担します。誰かが私の口座で小切手を偽造した場合、それは私の署名ではなく、銀行に私の口座からの引き落としの義務を与えていません。ですから、彼らが偽造された署名に不注意に依存している場合、それは彼らの見張りです。  
さらなるロビー活動の後、ヨーロッパはeIDAS規制（910/2014）で法律を更新しました  
現在、多くのEU諸国では、このような署名を使用して、許可するのではなく、税金を申告するように求めています。  
数十の署名作成製品が正式に認定され、市場に投入されました。  
欧州委員会は、政府がすべての署名の検証を開始できるように、参考実装を正式に提供しました。 2019年にバグが発見され、市民が他の人になりすますことができるようになりました[429]。  
26.5.3何がうまくいかない  
古い落とし穴は、その信頼性について十分な懐疑論を適用せずに、紛争の一方のシステムから抽出された証拠に依存しています。  
銀行口座からの不正な引き出しについて苦情を述べた後、詐欺未遂で男性を誤って告発し、誤って有罪判決を受けました。  
銀行はこれを拒否し、銀行の陳述は容認できないものとされ、訴訟は崩壊した。  
私が知っているコンピュータ証拠の最悪の失敗は、オア作戦でした。  
ほとんどのカード所有者がおそらくカード詐欺の犠牲者であることに警察が最終的に気づくまで、2000年代初頭に約3,000の家が襲撃された。  
 そして政治のために（トニーブレア首相自身が襲撃を命じた）  
そのため、数千人の男性が数か月、さらには数年にわたって命を落としました。警察が暴力を振るったり隠蔽したりする悲しい話は、ダンカンキャンベルによって[375、376]で伝えられています。  
彼らのうち少なくとも1人、ジブラルタルのイギリス軍の指揮官であるコモドール・デビッド・ホワイトは無実だったように見えます[886]。  
アメリカはこの事件をはるかにうまく処理した。  
実際の児童虐待に対する100以上の有罪判決が続いた。  
会社は、誰かがそれらを保存するために積極的な行動をとらない限り、一定期間後にすべての電子メールが破棄され、他の多くの会社もそれに倣ったという方針に反応しました。しかし、コンピューター科学捜査の最大の問題は、常にまったくのお金の不足でした。  
彼らは、白い粉のすべてのラップをラボに送り、それが違法かどうかを確認する余裕さえありません。  
したがって、強力な法的手続きが開発される前であっても、キオスクを使用するという大きな圧力がかかります。  
司法教育も問題です。確率論を理解している裁判官はほとんどいません。実際、英国の控訴裁判所は、ベイズの定理に基づく証拠の分析を受け入れることを拒否しています。  
  
プライバシーとデータ保護は、米国とヨーロッパが別々の道を歩んできた一つの主題です。  
 通常、拡散した関心よりも優先されます（個人が私たちの個人情報を管理したいという欲求など）  
集中した関心が議員に働きかけ、彼らが設立した規制当局を捕まえようとするため、救済策は不完全です。  
結果として生じた湾岸は、2014年5月、米国の科学技術諮問委員会（PCAST​​）の大統領評議会で力強く強調されました  
このレポートは、GoogleのEric Sc​​hmidtとMicrosoftのCraig Mundieを著者として含み、クラウドサーバーに接続されたスマートオブジェクトでいっぱいの世界の絵を描きました。 。  
センサーが多すぎるため、センサーにプライバシーコントロールを課すことはできないと主張しました。中央のサービスアグリゲーターに課せられるべきではないこと。したがって、統制は情報の使用方法に依存する必要があります。  
スペインの弁護士、マリオコステヤゴンザレスは、彼の名前を検索すると、取り押さえられた家のオークション販売に関する2つの古代の新聞報道をもたらしたと不満を述べていました。  
グーグルは新聞の内容を報道しているだけだと主張した。  
Googleと他のオンラインサービスプロバイダーは、「処理された目的に関して、不適切、無関係、またはもはや関連性がない、または過度である」という検索結果について人々が不満を述べ、それらを削除してもらうメカニズムを設定する必要がありました。 。  
Googleの支持者は、これは米国での言論の自由の権利を妨げると主張しています。  
   
プライバシーを損なうテクノロジーへの恐怖は最近の進展ではありません。  
銀行、徴税人、福祉機関が1960年代初頭にコンピューターを使い始めた後、すべての取引を照合して分析できれば、人々はプライバシーへの影響を心配し始めました。  
これは、ほとんどのヨーロッパ諸国のゲシュタポと東部の共産主義秘密警察の生きた記憶を考えると、人権問題となった8。  
テクノロジーが変化する速度のため、成功した法律はテクノロジーに中立でした。  
 個人データのユーザーは誰に報告しなければならず、誰が不適切な処理をやめ、それをやめるように彼らに指示することができるか。  
時間が経つにつれ、多国籍企業による処理も問題になり、人々は純粋に地方または国のイニシアチブはそれらに対して効果がない可能性が高いことに気付きました。  
厳密に言えば、この条約は自発的でしたが、多くの州がデータ処理市場へのアクセスを失うことを恐れてそれに署名しました。  
最高裁判所は、結果として誰も逮捕されなかったとしても、3万人以上の男性学生またはイスラム教徒の大多数の国からの元学生にファイルを作成するという憲法違反の2001年の警察の行動を認定しました。  
詳細とクレジットカード購入パターン。  
ほとんどすべての商用データがカバーされています。  
実装の質は大きく異なりました。  
戦後の憲法にプライバシーの権利を書いていたドイツでは、データ保護機関が適切な法執行機関になった。  
1990年代初頭までに、国内法の違いにより貿易に障壁が生じていました。  
したがって、データ保護は最終的に1995年にデータ保護指令[647]でEU法の地位に引き上げられました。  
また、契約または条約によって実施される同等の管理がない場合、個人情報が米国などの「データ避難所」に送られるのを防ぐことにも着手しました。  
たとえば、データ管理者は、自分自身が再識別に必要な補助データを所有していない限り、軽く匿名化された情報はもはや個人情報ではないと偽ることができます。アイルランドの執行はさらに弱かった–過去50年間のその産業戦略は、米国企業の欧州本部を誘致することであった。  
フランスやドイツなどのプライバシー法が厳しく、苛立たしい国々は、一般データ保護規則（GDPR）を要求しました。  
これは、これまでで最も多額のロビー法案であり、欧州議会の委員会で3,000を超える改正が議論されました[82]。それは9行目で助けられました免除があると期待する1つのケースでは、そうではありませんでした。ラップトップまたはPCに個人を特定したメモを付けていたジャーナリストは、この情報のコピーをオンデマンドでデータ主体に渡す責任を正式に負っていました。  
GDPRはすべてのEU加盟国で直接効力を発揮し、英国またはアイルランドが抜け穴を導入するためのゆがみの余地をなくしました。しかし、ロビイストはすでに規制のかなりの数を獲得しています（特に科学的であろうとマーケティング的であろうと、「研究」のために）  
通常のビジネスへの主な影響は、個人情報のすべての使用を文書化し、それぞれの法的根拠を事前に書き留めることを強制することです。一度挑戦したものを試してみるだけでは十分ではありません。  
ロビイストによって挿入された多くのカーブアウトにもかかわらず、GDPRは、規制当局に反発するためのツールを提供しています。  
同意を強制することも推定することもできないという事実は大きな問題になる可能性があり、パイプラインにはさらに多くのケースがあります。  
26.6.2米国のプライバシー規制  
州法と連邦法のパッチワークがありますが、それらはアプリケーション固有で断片化されています。  
いくつかの規制の島には、1970年の公正信用報告法が含まれており、これは信用情報の開示を管理し、ヨーロッパの規則に広く類似しています。ワシントン州の新聞が米国最高裁判所に指名したロバート・ボーク裁判官のビデオレンタルの歴史を発表した後に制定されたビデオプライバシー保護法または「法案」。ドライバーのプライバシー保護法は、女優レベッカシェファーが自分の住所を見つけるために私的な目を雇った取りつかれたファンによって殺害された後、DMVレコードのプライバシーを保護するために制定されました。医療記録を保護する健康保険の相互運用性と説明責任に関する法律で、第9章で説明しました。  
いくつかの不法行為はまた、驚くほど多くの状況で民事訴訟の根拠を提供しています。調査については、Daniel Solove [1801]を参照してください。  
2007年、ストアチェーンTJ Maxxが4570万人の顧客のクレジットカード情報を盗んだことが判明しました[1159]。 2010年、アルバートゴンザレスはこのために20年の禁固刑を科されました。この違反により、同社は8億ドルの損害を被ったと考えられています。  
20年の監査を受けること[181]。  
米国11と他の地域12の両方で、Cスイートの大虐殺が続いており、サイバーセキュリティを着実に企業の課題にまで引き上げています。  
。  
投票はケンブリッジアナリチカスキャンダルに続いて行われ、8700万人のユーザーのFacebookデータが知らずに、または同意なしに収集され、2016年の選挙キャンペーン中に行動広告をターゲティングするために使用されました。  
CCPAはヨーロッパのデータ保護法に多少似ています。消費者が個人情報の削除を要求し、その販売をオプトアウトし、第三者への転送を可能にする形式でアクセスできるようにします。  
CCPAは、州検事総長だけでなく、私的措置によっても執行できます。  
しかし、アメリカだけがここで真剣なプレーヤーではありません。  
26.6.3断片化？  
これを解決する最初の試みは、セーフハーバー協定でした。これにより、アメリカまたはインドのデータ処理業者は、ヨーロッパの顧客にヨーロッパの法律を遵守することを約束しました。  
しかし、それは彼らの権利が侵害されたと感じたEU市民に実用的な手段を残しませんでした。  
スノーデンの啓示に続いて、彼はアイルランドのFacebook（そのEU本部）のためにそれを主張した  
欧州司法裁判所はこれに同意し、2015年にセーフハーバーの原則を破棄しました。  
12Dido Harding of TalkTalk、英国、2017年。 2019年、シンガポールのIntegrated Health Information SystemsのBruce Liang氏。また、VWのMartin WinterkornやAudiのRupert Stadlerも数えることができる。彼らは自動車の排気ガスをハッキングする会社を主宰した。EU市民がNSAが彼らをスパイしたかもしれないと思うならば文句を言うことができる追加とオンブズパーソン[1474];マックスもこれを2020年7月に正当に打倒した欧州司法裁判所に提出した[1683]。  
裁判所はまた、プライバシー当局が苦情を受け取った場合に行動を起こす義務があると決定しました。  
米国でデータを処理する多くの企業は、その間に契約に戻っており、顧客はビジネスを行う前に個人データが共有されることに同意する必要がありました。  
、およびECJは標準の契約条項（SCC）の継続的な使用を許可しました  
しかし、これは簡単ではありません。  
米国の法律が米国の土壌に関する外国人のデータへの自由なアクセスを提供し、スノーデンの開示が体系的な使用を文書化している場合（およびEU法の観点からは、虐待）、米国企業がどのように適切性を確立できるかを理解することは困難です。  
したがって、これは実際の戦いに発展しており、世界のサーバーファームがどのように、どこに配置され、制御されているかについて、実際の結果が出ています。  
そしてアメリカの世論はヨーロッパとそれほど違いはありません。ほとんどのアメリカ人は個人データが今は安全ではなく、監視資本主義のリスクが利益を上回っており、彼らが何が起こっているのか理解していないこと、彼らがコントロールできないことを考えていますそして、企業も政府も虐待の責任を負いませんが、彼らには代替手段がないだけです。  
一方、データ保護法は、不正使用に対応する方法を提供する新しい分野に力を入れています。  
マーケティングおよび政治的宣伝における多くの現代の慣行にはデータ保護法に基づく違反が含まれているため、これは規制の対象となります14米国の大量監視に対してビッグブラザーウォッチが提起した欧州人権裁判所で係争中の訴訟もあります[420 ]、それは大会議所に上訴を与えられました。  
15英国の罰金は、GDPR以前のデータ保護法で許可された最大値でした。それ以来、最大は被告の離職率の4％であり、これによりヨーロッパのペナルティはアメリカのペナルティと一致するはずです。  
米国の同等の法律は、プライバシーポリシーやユーザーのプライバシーに関する以前の合意に違反する企業を処罰するためにFTCが広告真実法を使用することです。そしてフェイスブックはやがてFTCから50億ドルを調達された。  
  
情報は弱いものから強力なものへと流れる傾向があり、その力を増大させ、他の人がそれらを説明することを保持することを困難にします。  
知識は永遠に無知を支配します。そして、自分の総督になるつもりである人々は、知識が与える力で武装しなければなりません。  
より過激なバージョンが試されました：税申告書はアイスランドといくつかのスイスのカントンで公表されます、そして、金持ちが宣言された低い収入がもたらす社会的地位の喪失を恐れているので、慣習は回避を減らします。  
彼は、データ取得、送信、保存のコストが下がることで、広域監視技術が当局に利用できるようになると考えているため、唯一の真の問題は、他の人にも利用できるかどうかです。  
彼は、たとえばすべての銀行口座を含む、本質的にすべての情報が開かれているべきだと主張しています。  
 ソーシャルメディアはしばしば私たちをその方向に押しやっているようです。  
しかし、透明性は興味深い闘争につながります。  
しかし、Web検索エンジンが存在するようになった今、そのような法律を施行するにはどうすればよいでしょうか。  
 グーグルスペインの事件は私たちに答えを与えます：有罪判決が失効した人は検索でそれを抑制する権利がありますが、どこを見ればよいか知っている人のために新聞のアーカイブに残るかもしれません。  
17トニー・ブレアは後でそれを彼の最大の間違いだと説明した。  
もう1つは、元児童の性犯罪者の監視であり、一部の州では犯罪者の登録簿の公開を義務付けており、日曜日の新聞による以前の犯罪者の名前と少なくとも1人の無実の人物がリンチ。  
その他の例については、推論セキュリティに関するセクション11.1を参照してください。  
26.8まとめ  
政府の最大の懸念は、それをドルで測定すると知性です。典型的な政府は、サイバー犯罪に対抗するよりも、実際および潜在的な敵に関する情報収集に100倍以上のお金を費やしています。ただし、Snowdenの啓示により、世界中の米国のデータ収集の規模、および同盟国に対するFive Eyesの活動の規模が明らかになったため、バランスは変化し始め、その影響はプライバシーとデータ保護法を通じて広がっています機関自体への影響はほとんどありません。  
 一方、ポリシーの効果は、プライバシーをより多くの人々にとってより目立たせることにより、「監視資本主義」の過剰の一部を抑制することになるかもしれません。  
他の国々もそれに倣い始めています。  
インターネットのおかげで、中国まで行かない国が破壊的なコンテンツを検閲することはさらに困難になっていますが、10年前の楽観的な見方の多くは、アラブの春の失敗で消滅しました。  
AOLがユーザーをスカンソープに住むことを禁止してから25年になります。大規模なフィルタリングでは、著作権、過激化、嫌がらせ、または偽のニュースについて話している場合でも、依然として多くのポリシー問題が発生します。  
これは、私たちのセキュリティ、私たちの自由、そして私たちの生活の質を損なうコンピュータとネットワークの悪用ツールの急増につながりました。  
オンラインの危害を軽減しながら監視エコシステムを理解して後押しすることは、直接的に、または私たちの執筆と教育を通じて、公の生活に関与する能力を持つセキュリティエンジニアにとって最優先事項です。  
個々の学者はマスメディアで全国の指導者と競争することを望んでいませんが、長年にわたるデータと知識の慎重な蓄積は彼らの言い訳を損なう可能性があり、また損ないます。  
研究上の問題技術政策には、科学、工学、心理学、法学、経済学の間の複雑な相互作用が含まれます。  
2002年以来、私はセキュリティ経済研究コミュニティの構築に尽力してきました。 2008年以来、心理学者、人類学者、哲学者も参加するために、セキュリティと人間の行動に関する年次ワークショップを開催しています。  
歴史家、社会学者、政治学者はどこにいますか？  
 参考資料テクノロジーポリシーの議論が現実から切り離されるのは非常に簡単であり、多くの恐怖が注目を集めてお金を得るために立ち上がっています（「サイバーテロ」など）。  
エンジニアは、R.V。などの経験豊富な内部関係者が作成した資料から、主要なソースを探す必要があります。  
Brexit国民投票および2016年の米国選挙における情報戦テクニックの使用については、キャロルカドワラの映画「グレートハック」は必見です。  
私のウェブサイトに、ヨーロッパの観点からの暗号戦争の歴史のビデオがあります。  
オンライン検閲に関するリソースには、国境なき記者団が含まれます。国境なき記者団は、ブロガーとサイバー反体制派のためのハンドブックを発行して、センサスを回避する方法と、ブログがリベラルでない国々でメディアを開拓するのにどのように役立ったかについての多くの事例履歴を掲載しています。 [1594]。  
初期のコンピュータ犯罪事件の履歴については、Peter Neumann [1429]およびDorothy Denning [539]を参照してください。  
プライバシーとデータ保護のトピックに関しては、膨大な文献がありますが、私が知っている簡潔な最近のガイドはありません。  
炎症性コンテンツとプロパガンダのフィルタリングに関するポリシーの問題については、私にとって2つの最も示唆に富む本はTim Wu [2050]とYochai Benkler [227]によるものであり、Facebookの元CISO Alex Stamosは現在、テクノロジー企業について議論しています。政治広告のフィルタリングのビュー[999]。