。  
自由への最大の危険は、熱心な男性による陰湿な侵入に潜んでいます。  
–アクトン卿弁護士とエンジニアの議論は怒っている幽霊のように別のものを通過します。  
1はじめに政府は、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、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、テロや反乱から国家の戦略的および経済的優位性、有害または不人気なコンテンツの抑制、人権の維持に至るまで、多くの特定の政治的懸念の周りに具体化します。  
インターネットは、電気、蒸気エンジン、執筆、農業、そして石油など、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。  
 初期の頃には、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に開放されたため、多くのパイオニアが存在しました82026。  
 はじめにユートピアでした：私たちは、情報への自由な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にするだろうと信じていました。  
 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、現実的な影響を与えました。  
 振り子が2010年代に監視資本主義に逆戻りした一方で、COVID-19のパンデミックルックは、国家監視をもう一度増加させるように設定され、トレードオフはプライバシー対セキュリティではなくプライバシー対健康です。  
 2013年にエドスノーデン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深刻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、より原始的ですが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、他の州によるさまざまな種類のサイバー兵器の取得が急増しました。  
多くの厄介な問題があります。  
9/11以降、通信の大規模な監視から、裁判や事件のない拘留まで、権威主義的な措置が次々と見られてきました。  
 自由を守るより良い方法を見つけられませんか？そして、どのようにしてコアバリューを再主張し、擁護することができますか？2つ目は、安全保障の政治経済です。  
 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、今後も続くでしょう。  
 左と右の政治家は、セキュリティ機関とマスコミによって煽られて、恐れの文化を煽りました。  
セキュリティ技術の議論は、竹や脅迫的な議員によく使用されます。  
 しかし、9月11日以降、これはすぐに28日に引き上げられ、その後、容疑者から押収されたPCのデータを解読するのが困難である可能性があるとして、90日が必要であると政府は述べました。  
1。  
 警察が「容疑者を90日間拘束する必要があるのは、ソマリ語の通訳者が足りないために必要だ」と言ったばかりの場合は、常識が働いていた可能性があります。議会は彼らに商業翻訳代理店からのsta useを使うように言ったかもしれません。  
 暗号法を理解する人々には、発言する義務があります。  
 すべての犯罪の約半分は現在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るリソースはごくわずかです。  
検閲に関してさらに問題があります。  
 虐待の深刻さは、殺人事件や児童強姦のビデオから、ヘイトスピーチ、レイプの脅威、ネットいじめ、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に至るまで、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。  
そのような議論は、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たときや、犯罪のライブビデオを共有するためにFacebookを使用したときなど、主要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、同社は業界がこれまで不可能、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、および社会的アドバイスのプッシュ[984]。  
プライバシー規制はすでに複雑です。S  
 ヨーロッパは非常に異なっています。一般データ保護規則は、監視に関する法律を制圧するために使用されてきた人権法に裏付けられた包括的な枠組みを提供します。  
 （この規制力が安全にも着実に拡大されるという強い兆候がありますが、保証に関する章に残します。  
セキュリティエンジニアリング822ロスアンダーソン26。  
 監視26。  
 2つはさまざまな方法で相互作用します。  
 中国のように、当局に完全なアクセスを与えることを拒否したため、これらの企業は禁止されている。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盗んだり、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。  
26。  
1政府の盗聴の歴史ルーラー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「コードブレーカー」[1001]に記載されています。  
 ほとんどのヨーロッパでは、電信サービスは政府が所有するポストオーシャンの一部として設置されました。イギリスでは、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。  
 米国では、ウエスタンユニオンが最初の全国的な産業独占であり、19世紀まで市場を支配していました。  
電話の発明はプライバシーをめぐる争いにつながりました。  
 1967年、裁判所はカッツ対米国で逆転し、改正は場所ではなく人々を保護するとの判決を下しました。  
 1978年、ニクソン政権の人権侵害に対する調査が行われた後、連邦議会は、国家のセキュリティの盗聴を規制する連邦情報監視法（FISA）を可決しました。  
 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により、モデムのアダプティブエコーキャンセレーションなどの技術開発と同様に、当局による盗聴機能が損なわれ始めました。  
2。  
 1999年までに、1,350件の裁判所命令[634、1257]に続いて2,450,000件を超える電話での会話が合法的に行われました。 2017年までに、盗聴の注文数はほぼ3倍の3,813になりましたが、94％が携帯電話などのポータブルデバイスに対するものでした[1927] 1。  
9/11以前でも、一部のアナリストは、許可された盗聴と少なくとも同じ数の無許可の盗聴があると信じていました[558]。  
第二に、諜報機関の裁定取引があります。NSAが保証なしでアメリカ市民を盗聴したい場合、彼らはそれを行うために味方を取得し、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、NSAはGCHQを取得して、2で説明したように、Googleデータセンター間のリンクをタップしました。  
 第3に、一部の国では、加入者の1人が同意した場合、盗聴は制御されません。したがって、電話ボックスからの通話は自由にタップできます（電話ボックスの所有者は正規の加入者です）。  
 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ます。  
しかし、たとえ社会的な見方を2倍または3倍にする必要があるとしても、民主主義体制は独裁的なものよりもはるかに少ない盗聴を使用します。  
 また、頻繁な路上検問所から、少数家族の家でのビレッティングパーティのメンバーまで、労働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）[1927] 。  
 盗聴はオランダでは非常に一般的です。外出先で10分の1で最大1,000タップです1関連法は18 USC（US Code）2510–2521ですが、FISAの外国情報収集に関する規制は現在、米国法で50 USCとして規定されています。 1801–1811。  
2。  
 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日常的です。  
 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。代わりに、警察のUseroomのバグとコンピュータの悪用。国際電話は何十年にもわたって定期的に記録され、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年のムンバイでの大虐殺の後、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通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年の米国の警察機関の支出はわずか51ドルでした。  
 CALEAの実装は5億ドル以上かかり、それは2007年にVOIPに拡張される前でした。  
 2010年代には、人々が携帯電話などの物理的なプラットフォームからFacebook、Skype、Signalなどの仮想プラットフォームに移行したため、状況はさらに厳しくなりました。  
 たとえば、10年前、英国の警察が3つの類似したレイプを調査していた場合、3サイトすべてに存在する携帯電話を探すために、セルサイトのダンプを組み立てるために電話会社に数千ポンドを支払う必要があったかもしれません。  
 これは、警察と諜報活動の両方の性質を変えます。  
 9/11攻撃の43日後、議会は愛国者法を可決しました。これにより、法執行機関が保存された記録（金融、医療、政府の記録を含む）、所有者の知らないうちに家や企業を「こっそり」検索すること、およびFBIが国家安全保障書簡を使用して、財務、電子メール、電話の記録にアクセスできるようにする。  
 2005年12月、New YorkTimesは、ブッシュ大統領が2002年のテロの疑いがある米国居住者の無法盗聴を強制する秘密の命令に署名したことを明らかにした[1606]。  
 CDRプログラムは、1992年にブッシュ大統領の下でDEAによって開始され、アメリカ人による特定の国への通話と特定の国への通話がターゲットになりました。それは9/11の後に彼の息子が米国内のすべての電話のためのCDRの収集を許可したときに増加しました[877]。  
 NSAはセキュリティエンジニアリング825ロスアンダーソン26に圧力をかけました。  
 機密扱いの契約を差し控えると脅迫することにより、Qwestは監視するため、Qwestの弁護士はNSAにその提案をFISA裁判所に提出するよう求めました  
 それ以来、9/11以前にもデータを引き渡すようにQwestに圧力をかけていました[768]。  
2007年11月、ワシントンポストは、NSAが純粋に国内の電話とトラフィックデータの多くを利用し、サンフランシスコのAT＆Tのピアリングセンターを利用してインターネットトラフィックにアクセスしたことを明らかにしました[1377]。  
 （これは両党を分割し、上院議員のオバマとファインスタインが改正を支持し、上院議員のマケイン、バイデン、リード、リーヒー、クリントンはそれに反対した。  
2。  
 通信セキュリティの章で、警察がこのようなデータを使用して犯罪者の連絡先のネットワークを追跡する方法、および犯罪者がプリペイド式携帯電話やPBXハッキングなどの手法を使用して無害なトラフィックに信号を埋め込む方法について説明しました。  
 定規は長い間、郵便が規制されていたとしても、容疑者の特派員を追跡するために郵便を制御してきました。  
 一部の国では、封筒の裏面に返信先住所を記載することを要求する法律を可決したことによる扇動の脅威について心配しました。  
 第一次世界大戦は、敵のラジオトラフィックの量を測定することで、それを簡単に解読できなかったとしても、どの程度の情報を収集できるかを戦闘員に教えました[1001、1380]。  
この本の最初の版を書いたとき、ペンレジスター（対象の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）に対して4886の召喚状（および4621の内線）があった一方で、1998年に承認された1,329の盗聴アプリケーションが米国にあったことに気付きましたトラップアンドトレースデバイス用の2437召喚状（および2770拡張子）（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）。  
 たとえば、Bell Atlanticは、1989〜92年に25,453件の召喚状または213,821件の顧客の通行請求記録の裁判所命令に対応しましたが、NYNEXは、1992年だけで未記録の顧客数をカバーする25,510件の召喚状を処理しました[402]。  
2。  
NSAは2006年に「国境内で行われたあらゆる通話のデータベースを作成する」ことを望んでいたため、非合法収集の期間中、9月11日以降、統計は暗くなりました。テロ[395]。2018年4月のレポートは、2017年のいくつかの図を示しています。これらは国の安全保障問題のみに関連しますが、コンテンツとトラフィックデータのバランスについていくらかの感触を与えます。  
 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（e。  
 一方、電子メールの召喚令状）16,924人の非居住者（トラフィックデータなど）が56,064人の非居住者とともに取得されました。  
現在、米国の諜報機関は、人間のアナリストがそれを見たときに、通信が「傍受」されていると見なしています。ソフトウェアによる分析はカウントされません（英国の法律では両方がカウントされます）。  
3。  
 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、そしてすべてのこれらの直接の連絡先を調べ、例外的に3番目の分離度にまで及ぶソフトウェアを使用します。  
 これらの連絡先は、宗教的過激派、右翼のヘイトグループ、組織犯罪など、さまざまな容疑者リストの何百万もの名前と比較され、アナリストは既知の容疑者とのつながりを理解します。  
）そのため、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ているわずか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彼らのコールデータレコードをソフトウェアによって見られました。  
それでも、（FISAによって修正された）愛国者法の第215条が無効になることを許可することについて、議会で長い議論がありました。  
 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。  
 最も集中的に収集されたのは中東でしたが、スノーデンは、ロシアのロシア人よりもアメリカのアメリカ人で収集された記録の方が多いと述べています[756]。  
2。  
 92];全体として、1日に200億のイベントが収集されます[816、p。  
ただし、機密解除されたレポートでは、米国のNSA通話データレコードプログラムの費用は1億ドルを超えていましたが、リードは2つと有意な調査は1つしかありませんでした[1656]。  
 スーザンランダウとアサフルビンは、4gモバイルネットワークでは、従来のCDRでは発信者と着信者の両方を確実に識別することができないと説明しました[1126]。  
特定の犯罪捜査における対象を絞った収集については、18 USC3123 [1925]の下で、捜査官は単に「そのような設置および使用によって取得される可能性のある情報が進行中の犯罪捜査に関連している」ことを治安判事に証明する必要があるだけです。  
 CALEA以来、サブスクライバーが電子メールメッセージを送信したアドレスなどの通信データには依然として令状が必要ですが、基本的な通行記録はサブポエナの下で取得できます。サブスクライバーは通知を受ける必要がなく、命令に裁判所による監督はありません。作られました。  
 最近は何も見つけることができません。  
 英国は、2006年にEuropeanUnionのデータ保持指令を推進しました。その下では、加盟国は、IPアドレスと、送受信されるすべての電子メール、電話、テキストメッセージのタイミングを含む電気通信データを6か月から24か月間保存し、メークこれは法執行機関と諜報機関が利用できます。  
英国では、通信データへの的を絞ったアクセスには、警官の電話会社またはISPへの通知のみが必要であり、令状は必要ありません。また、米国と同様に、幅広い公共機関にデータを提供できます。  
 国会議員とデイリーテレグラフに売却されたすべての費用請求のコピーを邪悪な人物が持ち寄ったとき、運命が介入しました。  
 （通信データベースを宣伝していたJacqui Smith内務長官の悲劇的な話をセクション8で伝えました。  
上記5。  
セキュリティエンジニアリング828ロスアンダーソン26。  
 監視欧州裁判所がデータの保持を取り下げ、スノーデンがGCHQによる非常に好ましくない活動を明らかにした後、英国は2014年のDRIPActを通過し、GCHQが行っていたことは結局合法であると主張しました。  
 最終的に、EU離脱の投票を受けて、議会は調査権限法を可決しました。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。  
2。  
 当時は、完全な盗聴とコンテンツの録音が行われているか、通話データレコードからのトラフィックデータが使用されていました。  
 一部の人は、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などのURLです。  
com / search？q = marijuana + cultivation + UKには、検索エンジンに入力された用語と検索エンジンの名前が含まれます。  
 これは、英国政府が監視法を近代化した1999年に実際の問題となりました。研究者、NGO、業界は、結果として生じた2000年の捜査電力法の規制に「ビッグブラウザの修正」を適用し、通信データを通信マシンの特定に必要な情報として定義しました。 URLの場合、これは最初のスラッシュまでのすべてを意味します。  
 （セクション11で説明したことを思い出してください。  
3 AOLが一部の検索履歴をリリースしたとき、それらの多くは個人が簡単に識別できました。  
 2006年に最終的に裁判官は、部門は検索クエリを取得せず、元々求めていた50,000件のURLのランダムなサンプルのみを決定しました[2035]。  
 英国では、携帯電話の位置に関するすべての情報が交通量データとして数えられ、社会関係者はそれを簡単に入手できます。しかし米国では、控訴裁判所は2000年に、警察が携帯電話の場所の令状を取得した場合、それがアクティブなセルが十分であり、デバイスで三角測量を必要とすることを決定しました（警察が望んだ解釈）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るが、これは人権裁判所ではなく、欧州安全保障理事会の機関である829ロスアンダーソン26である。  
 監視はプライバシーを侵害します[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。  
 場所データは現在、COVID-19サプライヤーと疫学のより一般的な連絡先を追跡する目的で、多くの政府によって収集されています。  
26。  
4アルゴリズム処理コールデータの分析は、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の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。  
 商業および政府のデータ処理者が使用す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が2016年にリーセドルを倒して以来、多くの機械学習新興企業が存在し、法執行機関をより簡単にするために、かなりの数の目的があります。  
 テロリストは、人口の割合として非常にまれであるため、偽陽性で溺れることがない場合は、それらを「検出」するために使用するテストで異常な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Je↵Jonas氏は、次のように述べています。「テロリストの意図を予測するために人々の行動を調べる手法は、私が見る必要がある正確さのレベルに達するにはほど遠い。市民的自由の侵害エンジンにすぎない」[757]。  
2。  
2。  
 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は単に自然な制御ポイントになりました。  
 FBIのシステムであるDCSNetは非常に洗練されており、エージェントがポイントアンドクリックで参加電話会社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、不正確なユーザーがIPアドレスに関連付けられるように不正確なタイムスタンプを提供したりします。  
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、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、ISPでの盗聴は何も伝えません。  
 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、「インドの家族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の人々を雇用し、人々に信頼できるプライバシーの保証を与えるのですか？最後に、FacebookのようなCSPから入手できるはるかに豊富なデータの周りには多くの問題があり、非常に機密性の高いデータを大規模に収集するだけでなく、以前は不可能であった方法でトラフィックデータから機密性のある事実を推定することができます。  
2。  
2。  
 法執行機関や諜報機関による社会分析手法の使用、またはそのために公衆衛生機関による使用には、どのような統制が必要ですか？ （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。  
2。  
2。  
 これらはすべて青からのものではありませんでした。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と認定された匿名の元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、外国政府が過去に何をしているか、計画しているか、何をしているかをカバーしています。どの空軍がどこに動いているか、そして彼らの能力は何であるか。  
 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を監視することまで、すべての方法に及んでいます。  
 1974年、彼は同盟国がその戦争中にドイツと日本の暗号システムを解読することに成功したことを明らかにし[2031]、第二次世界大戦の信号インテリジェンスに関するさらに多くの本（Sigint）[438、1002、2007]に至った。  
 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盗聴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の最初の注目度の高い展示会は、1999年の欧州議会への報告で行われ[644]、ソ連崩壊後、EU加盟国がNSAの主要な標的になることを懸念していた[644]。 377]。  
2。  
冷戦中、ソビエトのレーダーと通信を理解し、場所を特定したり、妨害したり、欺いたりするという決定的な優位性を得ることを目的として、ほとんどの軍事行動は軍事的でした。  
 NSAの人員のほとんどは軍人であり、その部長は常に将軍または海軍大将でした。  
この巨大な世界的なシステムのシステムがまだお金の価値を与えるかどうか疑問に思うかもしれません。  
 しかし、19章で論じたように、イラクの武装勢力に対する電子戦争は生産性が低いことが判明した。  
 アナリストは、9月11日の直前に発表された記事で、「TheCIAには、中東のバックグラウンドで真に適格なアラビア語を話す人物が1人もいないでしょう。アフガニスタンの山に食べ物はなく、女性もいない。  
 そのようなことはしません。  
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約20年が経過しましたが、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、多くの場合、経済的およびその他の非軍事的スパイ活動を実施することにはるかに積極的です。  
 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購入することに満足していましたが、今日では米国よりもはるかに大きな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]。  
私の見解では、軍隊がその一部であることが多いように、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考えています。  
 問題は、そのようなリソースが存在する必要があるかどうかではなく、どのように説明責任を負うかです。  
 Snowdenrevelations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は両方の責任があります3オバマ大統領が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ましたが、彼の前向きな作業はトランプ大統領によって取り消されました。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。  
2。  
 あなたがNSAのディレクターであり、あなたのエンジニアの1人がWindowsのクールな新しいゼロデイエクスプロイトをやって来たと想像してください。  
20億中国人？これらの用語を述べると、答えは明白です。  
 同グループは、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。  
2。  
5。  
フランスとドイツの両方で、攻撃と防衛のために別々の機関が存在する国もあります。  
 英国では、監視の規模を認め、それに対する立法を制定するよう政府に強いたのは、ヨーロッパの裁判所だけです。  
 2019年、欧州人権裁判所は英国の警察に、その「過激主義」データベースから、犯罪歴のない94歳の抗議者であるジョンキャットが参加した約60件のデモの記録を削除するように命じました。 2024]。  
 別の側面はスケールです。  
政府によるデータへのアクセスに対する結果として生じる圧力は、1990年代の政府による暗号鍵へのアクセスに対する圧力と非常に似ています。これは、多くの政府（および産業と市民社会）にとって、監視と技術政策の問題に関する形成的な経験でした。  
2。  
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人として関与し、1998年に英国のインターネットポリシーシンクタンクである情報ポリシー研究財団を設立し、暗号と格闘しました。ポリシー、輸出政策、著作権および関連する問題。  
 次のいくつかのセクションでは、暗号化戦争の簡単な背景を説明し、その後、政府がインターネットにうまく対処できなかった方法について説明します。  
2。  
2。  
1暗号化ポリシーの裏話多くの国では、19世紀半ばに電信メッセージでの暗号技術の使用を禁止する法律を制定し、一部の国では承認済みリストにある言語以外の言語の使用を禁じていました。  
 時々、言い訳は法執行であり、人々が「公式な」送信に先立って競馬結果または株価を入手することを妨げたが、真の懸念は国家安全保障であった。  
第二次世界大戦中に信号インテリジェンスを用いて連合国が達成した計り知れない成功の後、イギリスとアメリカの政府は1946年に情報収集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。  
」[206]これらの交渉では、当局は、可能な場合は弱い暗号を使用するように申請者を誘導しようとし、より洗練されたユーザーに直面すると、システムに「バックドア」があることを貿易に知らせようとします（業界では赤い糸として知られています） ）これにより、トラフィックへのアクセスが可能になります。  
 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、ボウラー事件で学んだように、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、当局がイラク人がイラン-イラク戦争中に自分たちの交通を読んでいたと告げた。彼らは、NSAが平文を入手できるように改ざんされた暗号マシンを販売したとして彼を非難した。  
440億リアル–その後は約100万ドル–で彼を保釈したが、スイスに帰国した後、彼に発砲した。  
 1つの話は、Crypto AGの創設者であるBoris Hagelinが引退することを決定したときに、NSAの主任科学者であるWilliamFriedmanに連絡したというものでした。フリードマンは友人であり、アメリカ政府は第二次世界大戦中にヘーゲリンの機械を購入する大口顧客でした。  
 それが販売した機器は、定期的に赤いネジでした[1205]。  
2。  
 バウラーの話は、レスストレー[1837]による本で語られました。  
 彼らの機器のバックドアは、例えば1982年のフォークランド戦争中にアルゼンチンの通信を解読するために英国によって使用されました-その結果は、この作戦によって「決定されなかったとしても、実質的に影響を受けました」[970]。2。  
2DESと暗号の研究初期の銀行の暗号システムは質が悪いにもかかわらず、NSAは70年代に銀行セクターが野生に脱出でき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ず、情報収集のコストを押し上げることなく、どうすれば緩和できるのでしょうか？ソリューションはデータ暗号化規格（DES）でした。  
4。  
2、56ビットで十分かどうかについて議論がありました。  
NSAは当時、DESキー検索を行うための機構を持っていませんでした。それは後で来ました。  
 ローターマシンは稼働を続け、多くの場合、マイクロコントローラーを使用して再実装されました。 Crypto AGと他の入札可能なベンダーが引き続き成長しました。そして、交通は収穫され続けました。  
2番目のイニシアチブは、暗号学の学術研究を損なうことでした。  
 国防総省はコンピュータセキュリティの研究に資金を提供しましたが、暗号の研究を理論上のチャネルに転用しようとし、より実用的な公開された研究はすべて古いものであると主張しました。なぜ納税者はそれを2度支払うべきなのでしょうか？」DESに「罠」が挿入された可能性があるという示唆は、この脚本にうまく適合しています。  
1990年代半ばまでに、このラインは使い果たされました。  
26。  
7。  
 Af-ter AT＆Tは、暗号化セキュリティエンジニアリング836ロスアンダーソン26の米国国内市場への導入を提案しました。  
 NSAは、Di-e-Hellman鍵交換とトリプルDESを使用してトラフィックを保護しているはずの電話で、クリントン政権に別の標準を推進するよう説得しました。  
 この「エスクロー暗号化スタンダード」は、一般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]、この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した認証局は、Trusted Third Parties（TTP）と呼ばれ、セキュリティを破壊する可能性があるものとしての、信頼されたコンポーネントのNSA定義を多少強調しています。  
寄託を支持する人々は、暗号は守秘義務を提供し、守秘義務は犯罪者を助ける可能性があるため、それを打ち破る何らかの方法が必要であると述べました。  
 現実はより複雑でした[56]。  
 犯罪者に関しては、彼らは主に非破壊的な通信を必要とします–そして1990年代に戻って、電話を暗号化することはあなた自身に注意を向ける良い方法でした。  
 プライバシーに関しては、ほとんどの違反は内部者による許可されたアクセスの乱用に起因します。  
議論は急速に武器、つまり暗号が伝統的に制御されていたテーマである輸出規制に巻き込まれた。  
 米国のソフトウェア作家PhilZimmermannは、彼が書いたプログラム（PGP）がインターネットに「エスケープ」された後、大規模な陪審員が武器を追跡する前に引き取られました。  
 ブルース・シュナイアーのような他の人々は、言論の自由に対する憲法上の権利を行使する方法として、本に暗号アルゴリズムを印刷しました[1667]。  
2。  
 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キャンペーンに貢献した理由です）。  
 1999年、欧州連合の単一市場担当委員であるマーティンバンゲマンは、認証機関の強制的なライセンスを禁止する法律である電子署名指令を推進しました。  
2。  
 ドイツ人は、署名キーをエスクローすることにより、機関がメッセージを読むだけでなくそれらを偽造し、電子商取引および認証に対する信頼を一般的に損なうことになると反対しました。  
欧州の企業は、EUの輸出管理を物理的な商品からソフトウェアなどの無形資産に拡張する輸出管理規制を可決することによって米国の行政を弱体化させ、ヨーロッパの企業は米国の企業と同じ暗号ソフトウェアの輸出管理に直面しました[651]。  
 QuanticoのFBIの場所で政府機関と技術系メジャーの間の会議が開かれ、政府機関が製品やシステムに脆弱性を挿入することをもはや要求しないという合意に至りました。ソフトウェアの脆弱性がCERTecosystemに報告されると、DoDが後援するピッツバーグのSoftware Engineering InstituteにあるCERTに到達します。  
 通常、パッチサイクルには1〜2か月かかります。脆弱性の開示と製品テストの調整が難しい場合は、さらに長くなることがあります。NSAにバグを悪用するための時間を与えます。  
監視の問題は大部分が解決されており、ソフトウェアの著作権やデータ保護などの問題が将来の問題になると考えました。  
 NSAと他の機関は単に地下に潜入しており、商用暗号を弱体化させるために年間1億ドルの予算でBullullと呼ばれる秘密のプログラムを実行しており、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、キー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、通常は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。  
 英国政府の考えでは、全員の秘密鍵はセキュリティエンジニアリング838ロスアンダーソン26を使用してメールアドレスから生成されるというものでした。  
 監視GCHQによって生成され、部門のセキュリティマネージャーによって制御される機器に保管されたスーパーシークレットマスターキー。部門とGCHQの両方が、必要に応じてトラフィックを復号化できるようにします。  
 カスタマイズされた中央制御の需要は、予算を超えて何年も遅れて何百万も実行される、またはまったくまったく機能しない、侵略的なITプロジェクトにつながります。  
 コロナウイルスの流行により、キャビネットは既知の不安にもかかわらず、会議にZoomを使用していました。安全なビデオ会議システムは実際には存在していましたが、分類されたため、大臣が自宅に持ち帰ることはできませんでした。  
 技術面では、弱い暗号化の義務的な使用により、DVDのリッピングが容易になり、自動車の盗難が容易になり、Bluetoothのハッキングが容易になり、Iwork4を含む建物を含む何百万ものビルディングロックが簡単に破られます。  
 政策に関しては、ロシアの過酷な暗号管理法などの権威主義政府。イギリスは、1990年代半ばのJohnMajorのもとでの自由放任政策から、トニーブレアの2000年調査法（RIP）に移行しました。 2002年は、56ビットよりも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する場合、輸出許可を取得するよう指示しています5。  
26。  
8Crypto War 2 – Going SpottyThe Edward Snowdenによる2013年の開示は、暗号戦争の流行後の再開につながりました。  
 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規模な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、ニュージーランドの5つの目への貢献です[850]。  
 彼らは法的規制を回避していました。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、これは常に疑われていましたが、常に拒否されていました。  
4セクション4を参照してください。  
車の盗難、セクション5の1。  
2。  
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。イランにいる場合、私のウェブ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。  
2。  
これらすべてが行動に本当に影響を及ぼしました。  
 MicrosoftとYahooが続いた。  
 第三に、政策対話は管轄権などのより現実的な問題に取り組み始めた。世界の警察が関心を持っている資料のほとんどが、それにアクセスできる米国企業のサーバーに保管されており、どのような条件で使用されているのでしょうか。英国のような国々が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た一方で、他の国々はローカリゼーションに向かった。  
 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。 EuropeanUnion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、法執行機関がサイレント電話会議の当事者（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制する必要があると主張し始めました。令状。  
 Facebookの対応は、彼らが米国とEUのプライバシー法を遵守していたというものでした。関連するサービスセンターは英国ではなくアイルランドにあったため、ハニガンは英国の法律を利用して強制的に支援することはできませんでした。  
私の暗号学者の同僚と私は、私たちの分析の最新版である「Keys Under Doormats」の更新を書くように再招集しました。これは、1990年代のキーエスクローの提案に関する問題の多くが、キーではなくデータへの政府アクセスを義務付けた場合、新しい形式で戻ってくる[5]。  
 政府が設計者に、当面に普及している転送秘密、認証された暗号化、厳格なトランスポートセキュリティなどのセキュリティメカニズムを放棄するように強いられた場合、および、セキュリティで保護されたシステム間の多くの相互作用のため、それは悪いことです。現在の方法では、重大で予期されない副次的影響を伴う必須の脆弱性のリスクは、今でははるかに大きくなっています。  
 実際、Googleの盗聴システムを2010年に中国でハッキングしたことは、優秀な企業でさえ常に国家の行為者を排除できないことを示唆しており、そのハッキングはシステムセキュリティエンジニアリング840ロスアンダーソン26を狙っていた。  
 SURVEILLANCEGoogleは盗聴に対応するために構築されました。  
 管轄権に関しては大きな問題があります。  
 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関する多くの質問を引き起こします。その一部は、分析で詳しく説明しました[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、共和党はFBI（当時のトランプ、そして彼の候補はアップルのボイコットを求めていた）を支持したが、ほとんどの民主党とハイテク産業はティム・クックを支持した。  
4。  
3。  
Brexit国民投票に続く混乱の中で、新しい英国首相のTheresa May（内務長官は監視のタカであった）は英国議会を通じて調査権限法を推進した。  
 2018年、GCHQの2人の数学者であるIan LevyとCrispin Robinsonは、メッセージングサービスへの政府のアクセスがどのように機能するかを提案しました[1153]。彼らのアイデアは、GCHQがFacebookに令状を提示したときに、GCHQ公開鍵を静かにターゲットのキーリングに追加して、すべての通話に対して無言の会議参加者になるというものでした。  
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、これを行うべきではありません。  
2。  
2019年、Mark Zuckerbergは、FacebookがInstagramとメッセンジャーとのunifyingWhatsAppを使用することにより、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と発表しました[1439]。  
 10月、USSecurity Engineering841Ross Anderson26。  
 監視司法長官は、英国の内務大臣とオーストラリアの内務大臣に参加し、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、単一のプラットフォームでリスクを浮き彫りにし、将来のベンダーに特定して独自のルートを提供し、私たちの子供たちをグルーミングします。  
26。  
9輸出管理暗号戦争からの波及は、特にヨーロッパにおいて、以前よりも均一な輸出管理を課すことでした。こちらが簡単な要約です。  
 暗号解読製品は軍事体制に該当しますが、保護に暗号化のみを使用するソフトウェアは二重使用に該当しません。  
 米国企業は不満を述べ、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、ヨーロッパで風土病であり、英国をEUから離脱させる運動を促進した要因の1つです。  
 使用できるオープンな一般輸出ライセンス（OGEL）がありますが、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の研究では、電子ビームワークステーションを使用しています。これは電子顕微鏡のようなもので、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、トラックを切断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、輸出ライセンスを購入したときに取得する必要があり、7年後にはスキップしてライセンスを取得する必要がありました。  
 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す。これにより、科学者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サイトにあることを非常に注意深くすることです。これにより、パブリックドメインの免除を使用でき、セキュリティエンジニアリング842Ross Anderson26をクリックするのはその人物であるという事実に依存しています。  
 TERRORISMonエクスポートを実行するリンク。  
 いくつかのデジタル著作権NGOの人々が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、それはドイツ人の問題でした;ワッセナーは人権問題ではなく軍事問題のため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、ドイツの首相アンジェラメルケルは、監視機器をシリアに販売することを許可することを決定したこと、そしてそれが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付託され、静かに忘れられた。  
 GCHQは、暗号を研究する中国の学生に反対し、セキュリティサービスは、英国でaPhD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りたときにハルツームに適格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した。  
 私たちは「AcademicTechnology Approval Scheme」を取得しており、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。  
3テロリズムテロについての話は、特に9/11以来、監視とプライバシーに関する多くの政策を推進してきました。  
サイバーテロの話がありました。それは基本的には発生していませんが、暗号化されたチャットサービスとソーシャルメディアが、右翼の憎悪グループからイスラム国家までの犯罪組織に若者を仕掛けたり募集したりするために使用されているという本当の懸念があります。  
テロは、マヤ、セキュリティエンジニアリング843、ロスアンダーソン26など、対象の母集団を牛に感染させるために長い間使用されてきました。  
 テロリズムインカ、ウィリアム征服者。  
 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行いました。  
 冷戦中、ロシア人はIRAだけでなく、バ​​ーダーマインホフガンギンドイツおよび他の多くを支持しました。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援した。  
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？まあ、良いニュースと悪いニュースがあります。  
3。  
 1960年代と70年代には多くの反乱があり、一部は民族的、一部は反植民地主義的、一部はイデオロギー的でした。  
 冷戦の終結により、動機とお金が取り除かれました。  
 Paul CollierとAnkeHoe✏erによるWorldBankへの影響力のある調査では、1960〜1999年の戦争を調べ、それらが主に不満（高い不平等、政治的権利の欠如、民族的および宗教的分裂など）によって引き起こされたか、または貪欲によって引き起こされたかを確認しました。 （一部の反乱は他のものより経済的に実行可能です）[459]。  
 （確かに、シセロは2000年前に「無限の金は戦争の筋を形作る」と言った。  
 したがって、私たちは反乱に取り組む1つの方法を知っています。それは、彼らのマネーサプライを削減することです。  
26。  
2政治的暴力の心理学心理学、政治学、メディアの学者から得られる刺激は少ない。セクション3で影響ヒューリスティックについて述べました。  
5：人々が影響を与える場所、またはセキュリティエンジニアリング844ロスアンダーソン26。  
 TERRORISMemotion、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、その後の自動車事故で、ﬂ yではなく運転することを決定した後、おそらくそうしました：ﬂ yingから運転への移行により、その後の3か月で約1,000人の追加の死者が発生し、年間約500人それ以来[1677]。  
 トム・ピシュチンスキ、シェルドン・ソロモン、イェー・グリーンバーグによるテロ心理学の研究では、人々が死の恐怖にどう対処するかを検討した[1564]。  
 彼らは最初に性格調査票を与えられました。そこでは、半分は「あなた自身の死の思考があなたに喚起する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かったことを示しました：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ために準備されました。  
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]。  
 宗教（1950年代以来の最高レベルの教会への出席）、愛国心（プレジデントへの高い承認評価の形）、および一部の人々の偏見も含まれるのは自然なことでした。  
不思議なことに、彼らが死ぬことを思い出したとき、保守派とリベラル派の両方が外国人学生によって書かれた反アメリカのエッセイをより二極化した見方をします。ただし、最初に憲法を思い出した実験では、保守派はリベラル派よりも激しくスピーチを自由にする学生の権利を守る[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、最高のリーダーが行うことです。  
 他の人たちは、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。  
 IslamicSecurity Engineering845Ross Anderson26。  
 テロリスト過激派はテロリスト78と名付けられた。  
時間の6％。  
 おそらく、最近の最高の反応は、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反応したことでしょう。彼女は即座にテロと述べただけでなく、射手に名前をつけることを拒否しました。  
 いずれの場合も、メディアは[1335]に従いました。  
3。  
 彼はそれを彼の賞講演で述べたように、「経済学者はあたかも慈悲深い専制君主に雇われているかのように、政策助言の売り出しをやめるべきであり、彼らは政治的決定がなされる構造に目を向けるべきです。  
 彼らが生み出す利益ではなく支配のスパンによってランク付けされているので、社会主義者が帝国を築くのは自然なことです。  
 彼らの決定を理解するには、方法論的な個人主義が必要です。国の潜在的な利益や損失ではなく、個々の大統領、国会議員、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です。  
 しかし、これは政治的にはより困難です。  
 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、後者では同じようにしますが、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。  
 政治的結果は、政治的行動を制約するルールに大きく依存します。  
 憲法は政治ゲームの基本ルールを定めているため、重要です。  
 たとえば英国では、9/11への最初の対応はセキュリティサービスの予算を増やすことでした。しかし、この1億ドルは、本物の豚肉をセキュリティ産業複合体に提供しませんでした。  
 ワシントンのインサイダーは、同様の力学がイラク侵攻の決定に関与していたと述べた：2001年の侵攻セキュリティエンジニアリング846ロスアンダーソン26。  
 テロリズムアフガニスタンは成功しており、戦車、資本船、爆撃機、または防衛産業の大部分を組み立てるキャリアを費やしてきた国防総省の男爵にあまり役割を与えていませんでした。「死の商人」を非難した第一次世界大戦の余波でも同様のことが言われました。  
「出血した場合はリードする」とのことわざは、悪いニュースは良い新聞よりも多くの新聞を売る。  
 彼らは愛国心の一時的なブリップと、テロ攻撃が自然に仕掛けるヒーローの必要性を拾い上げ、増幅します。  
 そして、多くのソーシャルメディアプラットフォームの推奨アルゴリズムは、人々がプラットフォームに費やす時間とクリックする広告の数を増やすにつれて、恐怖と怒りを促進することを学びます。  
3。  
 9/11に対する世界的な反応は鋭く、4年後の2005年7月に4人の自爆テロがロンドンの公共交通機関で52人を殺害し、約700人が負傷しました。  
’6そして人口が学べば、政治エリートもそうなるでしょう。  
ケネディ大統領、ジョンソン大統領、ニクソン大統領、フォード大統領はテロを無視した。  
 彼の国務長官サイラスヴァンスは後に、米国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ました。  
 しかし、このエラーから離れると、ヒスティング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は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：それから爆発的な犯罪があった。  
セキュリティエンジニアリング847ロスアンダーソン26。  
 再選挙キャンペーンで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、テロ対策のための準備に費やす時間ははるかに少なく、その多くは効果的ではなく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主張して正当化しました。  
 テロのレトリックは、公衆衛生を犠牲にして治安機関を苦しめ、アメリカ、ヨーロッパ、インド、アフリカの政府は、中国、シンガポール、台湾、韓国の政府とは異なり、2003年にSARSの教訓を無視するようになりました。  
4CensorshipIは、第1版で「暗号化ポリシーに関する1990年代の議論は、匿名性、検閲、著作権をめぐる、さらに大きな戦いの試練になる可能性が高いと書いています。  
 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。  
 1380–1年にジョンウィクリチェが聖書を英語に翻訳したとき、彼が始めたロラードの動き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年のサイバー犯罪防止条約により、署名国は18歳未満の性的画像を禁止することを義務付けられました。  
 英国は、テロを美化することで若者を「急進化」させるウェブサイトを禁止しています。  
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はより簡単になり、ある場合には困難になりました。  
 歴史を変えるセキュリティエンジニアリング848ロスアンダーソン26。  
 ライブラリ内の物理的なコピーで構成されている場合、CENSORSHIPicalレコードは不可能でした。Amazonの電子書籍システムから主要なニュース組織のサーバーまで、少数の企業のサーバーに人間の知識を一元化すると、 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。本当に不愉快なオンラインの多くは、ソーシャルメディアに匿名で投稿した何百万人もの個人、新聞のコメントページ、嫌がらせや脅迫したい個人に由来しています。  
 10年前の中国には反体制派の言論を取り下げた何万人もの人々がいたが、今では数百万の市民ボランティアが消滅させた。  
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。  
4。  
しかし、当局は、あらゆる形の組織や人の連帯を党の支配の外に抑えることにおいて、着実に効果的になっています。中国には当時、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いて、「中国の大ファイアウォール」は、ポルノから宗教的素材、政治的異議まで、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[ 1469]。  
まず、境界防御があります。  
 TCPレベルでのディープパケットインスペクションは、「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。  
3暗号化されたサーバー名表示（ESNI）を使用したトラフィック。これにより、検閲者がトラフィックの送信先のサブドメインを通知するのを停止します。これは、7月の初めまでにトラフィックの30％を超えました[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。  
 今や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てきました。  
4。  
 言語は1つの障壁を提供しますが、強力な技術的な障壁もあります。境界の防御は、承認されていないサービスを使用するために中国の居住者が使用できる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ポリサがありました。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、人々に反社会的行動の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「対テロ戦争」と毛沢東主義の社会的統制の融合技術を開拓し、数十万人のイスラム教徒の抑留につながった。容疑者は定期的に祈るか、電話にVPNがあります。  
S  
したがって、中国はポピュリストでありながら権威主義的な手法を用いて、検閲の戦いに勝利しているようです。  
 プーチン大統領は、ISPに監視および検閲設備の設置を命じることを可能にする「デジタル主権」法に対抗しました。  
 この一連の暴動は2010年12月にチュニジアで始まりました。モハメドブアジジは、彼の商品を押収し、屈辱を与えた後、彼自身を激怒させました。  
 エジプトの政府も、リビアとイエメンの政府とともに崩壊した。エジプトのケースでは、Googleの従業員であるワエルゴニムは、麻薬取引に関与しているというビデオ証拠があったという疑いで、警察のベアタ男がアレクサンドリアで死亡した後、インターネット活動家に転向しました。  
バーレーンをはじめとする他の多くのアラブ諸国は、取り締まりを大幅に強化しました。  
 エジプトでは、1人の軍事独裁者が別の軍事独裁者に置き換えられました。リビアは混乱状態にあり、シリアと同様にイエメンは戦争に悩まされています。  
 アラブ諸国はインターネットを検閲します（ほとんどの発展途上国と同様）が、それらのインフラストラクチャは依然としてVPNまたはTorを使用してかなり簡単に破られます。  
セキュリティエンジニアリング850ロスアンダーソン26。  
 検閲アラブの春は技術の機能でどの程度でしたか。また、このことは、順調に進んでいるように見えたときに、FacebookやGoogleなどの企業によって2011年に発表されただけのマーケティングの誇大宣伝ですか。はっきりしない。  
 アラブ世界では、カタールのテレビ局アルジャジーラは、地域の他の場所での蜂起のニュースビデオを表示することにより、インターネットよりも多くの仕事をしたかもしれません。  
4。  
 一方、米国は言論の自由を憲法で保護しています。フランスとドイツもそうです。  
 フランスとドイツはどちらもナチスのメモラビリアの販売を禁止しており、ヘイトスピーチ（「Volksverhetzung」）は何十年もの間ドイツで犯罪となっています。  
サービス会社が悪いstu↵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しなければならない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撃つ麻薬集団など、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。  
 そのような方針を実施するプラットフォームは、地元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：WhatsAppなどのエンドツーエンドの暗号化チャットは検閲されるのではなく非公開であり、放送メディアは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ます7。それは他のものからよりもトランプ大統領からのヘイトスピーチをはるかに寛容であり、そして逆戻りは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。  
セキュリティエンジニアリング851ロスアンダーソン26。  
 CENSORSHIPleasantness [1438]。  
 また、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。  
 世界はそれらが弱者を無視している間、金持ちで強力な人による虐待を許しているのを見ます。  
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であり、「インタラクティブコンピュータサービスのプロバイダーまたはユーザーは、別の情報コンテンツプロバイダーによって提供される情報の発行者またはスピーカーとして扱われない」と述べられているため、プラットフォームはユーザーによって提供された悪い状態に対して責任を負う。また、プラットフォームを自由に残して、わいせつ、わいせつ、わいせつ、不潔、過度に暴力的、嫌がらせ、その他の不快なものを削除しました。  
 イノベーションを殺すことなく、どうすれば市民インターネットを手に入れることができますかセクション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、中傷、または違法な銃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か国以上の国の検閲官、検察官、裁判官として行動する米国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年代に最初のマスマーケット新聞が登場して以来、プロパガンダの歴史であり、恐ろしい犯罪報告と特許医薬品の広告が掲載されていました。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。  
 テレビが次であり、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、石鹸などを開発して眼球をつかみました。  
 彼は政治の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ます。左と中央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、学校やその他の場所で批判的思考とme-diaリテラシーを促進しており、すべての市民の仕事になっています。セキュリティエンジニアリング852ロスアンダーソン26。  
 CENSORSHIPは、除算を行うために設計されたスポットおよびカウンター情報に使用します。  
 教師や大学教授は、過激化するリスクがあると思われる学生を報告し、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ことを想定しています。彼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。  
 白人至上主義者は、英国の離脱キャンペーン中に英国議会の議員を殺害したとして、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弾圧することにあまり気を配っていません、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は結局刑務所ではなく、政府の中心に行きました。  
 私は、殺人の扇動に関する既存の法律を施行すること（およびキャンペーンのファイナンス、他の政治的資料を公開すること、警察に交通を最悪の場所まで監視させ、既存の法律をよりよく利用するように訓練することを望みます[ 642]。  
イスラム教徒の学生を対象とすることに関しては、これは犯罪学的証拠に直接反するものです。  
彼らは、理想、共同体、親族、思いやり、そして兄弟愛を授けた過激な説教者の影響を受けました。  
 マックスアブラームスによる研究でも、テロリストは主に社会的孤立を求めて彼らの運動に加わったことが示されています。そのため、政治活動家の中からではなく、孤独な若い男性から採用しています。実際、シリアに行ってDaeshに参加し、最終的にはクルディシュヤイルに行った多数の若者にインタビューした後、Lydia Wilsonが指摘したように、若い男性（場合によっては女性）がテロに参加することで自分の身元を見つけるプロセス集団や犯罪集団は、宗教、スポーツクラブ、ダンスバンドに参加してアイデンティティを見つけることと同じです[2022]。  
5。  
 社会的連帯を求めて極端な組織に加わる人々は、自分たち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。  
 最善のアプローチは、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、小規模な教育グループ、プロジェクトグループなど、さまざまな背景から何百人ものスポーツや学生と他人を知ることができます。社会の選択から、誰もがセキュリティエンジニアリング853ロスアンダーソン26。  
 科学捜査と証拠のルールは、所属するギャングを見つけることができます。  
26。  
 これは、最初の膨大な量のデータが原因で、過去20年間にますます問題になっています。第二に、その多くが携帯電話やラップトップなどのプラットフォームから差し押さえられているものの、ますます多くのものが事務処理を必要とするオンクラウドサービスで保持されており、かなりの遅延が発生することが多いという事実。  
 その結果、サイバー犯罪者から忍び寄るいじめっ子、過激派に至るまで、多くの悪意のある人々がほぼ完全に免責されてオンラインで活動しています。  
5。  
 2010年代にオンラインですべてが移動したことで、事態はさらに悪化しました。  
 容疑者はまた、ウェブメール、ソーシャルネットワーキングサイト、その他のサービスのために数十のアカウントを持っている可能性があります。  
証拠におけるデジタル資料の使用は、しかし、法律と経済学の両方に依存します。  
 つまり、信頼できるツールを使用してデータの証拠コピーを作成することです。行われたすべてを文書化します。また、見つかった私的資料（特権を持つ弁護士とクライアントのメール、または容疑者の雇用主の企業秘密など）を適切に処理する手段を持つこと。  
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移行しています。  
 一部の警察部隊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のように、令状なしに「クラウドフォレンジック」を使用しません）が、すべてのデータを取得して保持しています。  
5。  
 かつて警察がPCをオフにしていたため、検察や弁護人がハードディスクをコピーできるようになりました。  
 また、ラップトップが暗号化された状態で出荷され始めたため、リスクが増大しています。  
昔は、警察の調査に巻き込まれ、コンピュータが押収された人々や小規模ビジネスは、たとえ傍観者だったとしても、起訴されて最終的には無罪になったとしても、何年も待って取り戻すことができました。  
これらのサービスはまた、容疑者の資料が海外のサーバーに置かれている警察の生活をより困難にします。  
2。  
 彼らが犯罪現場にいて、警察の反対側にいる間、Facebookは警察とセキュリティサービスのデータを即座に提供しましたが、2人が射殺されて病院で拘留されると、リクエストは英国と米国の相互の法的支援を通さなければなりませんでした条約。  
 UKpoliceの職員は米国の法律を理解しておらず、フォームを正しく記入していないため、フォームが返送されることがよくあります。  
 だから、私たちは襲撃の後で警察があなたのデータを持っているがあなたは持っていない世界から、あなたがまだあなたのデータを持っているが警察が持っていない世界からあなたが協力しない限り、またはあなたがいない限り、時間と外交官の注目に値するほど深刻な悪者です。  
 これが実際に意味することは、あなたの電話が警察の法医学キオスクによってハッキングされ、あなたのメール、あなたの写真、あなたのFacebookおよびあなたの他のクラウドサービスへのアクセストークンを放棄することです。  
 他の人は、それは同意または追加の令状によってのみ取得できると考えています。  
 そして、ますます多くのデバイスが接続されたクラウドサービスとアプリを取得しています。  
 偶然にも、裁判所は、どのような証拠を使用できるかについてすでにいくつかのルールを持っています。  
5。  
5。  
 データが正確であるかどうかという工学的な問題だけでなく、コンピューターで生成されたデータが伝聞として認められないかどうかという法的な問題もありました。米国では、法律の大部分は連邦証拠規則に記載されており、803（6）では、コンピューターデータを、知識のある人がその時点でまたはその近くで作成した、または知識のある人が送信した情報から作成されたレコードとして、定期的に行われるビジネス活動の過程。  
。  
’英国も同様であり、コモンローの国（カナダ、オーストラリア、南アフリカ、シンガポールを含む）における電子証拠のルールは、Stephen Mason [1236]によって分析されています。  
 英国では、裁判所はメールが手紙のように書いているという見方をしました。署名の本質は署名者の意図です[2042、2043]。  
 2000年に、議会は電子署名のグローバルおよびナショナルコマース（「ESIGN」）法を制定しました。これは、消費者が何かに同意するすべての「音、シンボル、またはプロセス」に法的効力を与えます。  
 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力を与えました。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、銀行に口座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。  
 さらにローブバイイングが行われた後、ヨーロッパはeIDAS規則（910/2014）で法律を更新し、2018年以降、すべての組織が公共サービスを調査して電子署名を受け入れるように要求することで、採用のインセンティブを改善しようとしました。  
 使用するテクノロジーの認定に応じて、署名を「拡張」または「修飾」できる階層があり、手書きの署名が以前に必要であったあらゆる目的で、修飾電子署名を受け入れる必要があります。  
 使用された保証メカニズムセキュリティエンジニアリング856ロスアンダーソン26。  
 後で28項で説明するように、そのような製品に欠陥があることを証明するための法医学および証拠のルールは、多くの点で欠陥があります。  
7。  
 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年には、市民が他者になりすますことができるバグが発見されました[429]。  
5。  
 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。  
4。  
 銀行口座からの不正な引き出しについて訴えた後、詐欺の企てをしたとして、男性は誤って非難され、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。  
4。  
 米国郵政公社がテキサスのポルノサイトを襲撃した後、彼らは、子どもの性的虐待画像を購入するために使用されたと考えられる数十万のクレジットカード番号を発見し、そのうちの約8000は英国のカード所有者からのものでした。  
 副チームはこれらの資料の最初の分析で未熟なスタッフを使用し、習得に時間がかかりました。なぜなら、彼らはすべての押収されたコンピューターを迅速に処理するための法的能力を持っていなかったためです。カード詐欺（銀行に任せるのが望ましい）と政治的理由（トニーブレア首相自身が襲撃を命じた）を理解する。  
 一部の人にとって、警察が台無しにしたという啓示は遅すぎた。 30人以上の男性が、迫害に直面し、自殺しました。  
児童虐待を組織して写真を撮ったインドネシアとブラジルの暴力団は、真剣に追求されていなかったようです。  
 同じサーバーで約30万件の米国のクレジットカード番号が見つかりましたが、米国の警察は証拠ではなく諜報目的でデータを使用し、子供と一緒に働いている人々などの懸念のある容疑者を特定し、静かに調査しました。  
システムは、証拠を提供しないように意図的に設計されている場合があります。例としては、1990年代に米国政府との独占禁止法の戦いの最中に恥ずかしいメールが出た後にマイクロソフトが採用したポリシーがあります。6。  
 もう1つの例は、2010年代半ばにサービスファームがエンドツーエンドの暗号化を採用したことで、顧客のメッセージトラフィックにアクセスする必要がなくなり、何百人もの弁護士を雇って要求に対処する必要がなくなります。  
 諜報機関がコンピューターシステムから情報を抽出するために使用できるすべてのクールなトリックにもかかわらず、郡の麻薬捜査班は、時折のビッグケースを除いて、基本的なコンピューターフォレンジックを行うために予算を割くことがよくあります。  
通常のケースでは、携帯電話のフォレンジックキオスクが2016年頃に登場し、押収された携帯電話から大量のデータを低コストで入手できるようになるまで、協力的証人の電話でのメッセージのコピーなど、簡単に入手できるデジタル資料しか使用できませんでした。 。  
 そして、もちろん、専門家の訓練を受けていない通常の警察官による法医学ツールの使用は、正義の将来の流産のリスクを高めます。  
 数学を否定する法廷制度の不正からかなり離れているが、バグの結果である、または単に誤って伝えられているというコンピュータ証拠に直面した被告には、その無罪を証明する実際的な方法がないかもしれないという現実的な問題がある。  
6プライバシーとデータ保護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。  
 集中した利害関係者が議員をロビーし、彼らが設定した規制当局を捕まえようとするので、救済策は不完全です。  
結果として生じた湾岸は、2014年5月に米国で大統領科学技術諮問委員会（PCAST​​）が「ビッグデータ：技術的展望」[1546]を発表したときに力強く強調されました。  
 PCAST​​は、音声とジェスチャーインターフェースの普及により、すぐに地球上のすべての居住空間にマイクとカメラが搭載され、出力がエネルギー効率のために中央で処理されると警告しました。  
2週間も経たないうちに、欧州司法裁判所はこれに同意しませんでした。  
6。  
 彼はスペインのデータ保護当局に、これらの結果が古く、関連性がなくなったため、Googleにこれらの結果の提供を停止するように依頼するように依頼しました。  
 訴訟はECJに行き、ゴンザレスで支持され、誤って「忘れられる権利」と誤って呼んだ場合にメディアが色鮮やかに作成し、後に2018年からヨーロッパの一般データ保護規則に編入されました。  
 メカニズムは議論の余地があります。スペインのGoogle検索からGonz`alezの結果が削除されていますが、ヨーロッパの規制当局は世界中での削除を望んでいます。  
この亀裂はどのようにして生じたのですか？  
1ヨーロッパのデータ保護プライバシーを侵害するテクノロジーへの恐怖は最近の進展ではありません。  
 1960年代初頭に銀行、徴税人、福祉機関がコンピューターの使用を開始した後、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の影響について心配し始めました。  
 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部隊の生きている記憶を考えると、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。  
 通常、実際的な効果は、一般法がドメイン固有の膨大な実践規約を通じて表現されるようになることでした。  
 1980年にOECDによって公布された自主的な行動規範に続いて[1476]、データ保護は1985年10月に施行された1981年1月にヨーロッパ評議会会議によって確立されました[475]。  
 個人情報には特定の最低限の保護手段が必要でした。これは、一般に、識別可能な人間または銀行口座などのデータ主体に保存されているすべてのデータを意味します。8ドイツでは現在、プライバシーが憲法に根付いており、「戦争による戦争」さえ踏みにじっています。  
 そのような演習は具体的な脅威に対応する場合にのみ実行でき、予防策としては実行できないと裁定した[344]。  
6。  
 データ主体は、保持されている個人データを検査する権利を持ち、不正確な場合は記録が変更され、その処理方法を理解し、多くの場合、同意なしに他の組織に渡されることを防ぎます。  
 国家安全保障には免除事項がありますが、詐欺師が望むほど完全ではありません。銀行間支払い指示を処理するSWIFTからのデータが、データ主体の知識なしに国土安全保障省にコピーされていることが判明したとき、大きな列がありました。 ; SWIFTは最終的に米国でヨーロッパのデータの処理を停止することに合意しました[1485、1486]。たとえば、英国では、マーガレットサッチャーは恥ずかしがらなく、遵守することをできるだけ少なくしました。データ保護団体が設立されましたが、資金と技術的専門知識が不足しており、政府と業界の両方に多くの免除措置が提供されていました9。  
 オーストラリア、カナダ、ニュージーランド、スイスなど、他の多くの国では、1980年代から1990年代初頭にかけて同等のプライバシー法案が可決されました。スイスなど一部の国はドイツモデルに、アイスランドやアイルランドなど他の国はイギリスに続きました。  
一部の企業は、データ処理を米国に移すことにより、管理を完全に回避しました。  
 これは、以前よりも高い最低基準を設定し、健康、宗教、人種、政治的つながりなどの非常に機密性の高いデータを特に厳格に管理します。  
イギリスの実施は再び最小限であり、ヨーロッパの要件にはるかに及ばなかった[597]。  
 情報コミッショナーのオフィスは圧倒され、プライバシーに関する公共部門のアドバイザーとプライバシー執行者を同時に務めた結果、深刻な衝突を起こしました。執行部門は、助言部門で同僚から恵まれたシステムに対して行動を起こすことに消極的でした。  
 したがって、法人税が低いことに加えて、ダブリン政府はデータ保護事業所を人口10,000人未満の町ポーターリントンに置き、30駅しか与えず、調査結果を公表することを許可しませんでした。  
 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以上の改正が議論されました[82]。それは一線を越えて助けられました9あなたが免除があると期待する1つのケースでは、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正式に提供する責任がありました。  
6。  
 GDPRはすべてのEU加盟国に直接影響を及ぼし、イギリスまたはアイルランドが抜け穴を導入するためのリグルームを削除しました。しかし、ロビイストはすでに規制に参加している人々をかなり多く獲得しました（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）。  
 情報集約型ビジネスの場合、その影響はより重要になる可能性があり、Facebook幹部が規制を改正するためにロビー活動を行った方法についての興味深い開示がありました-ブリュッセルでの擁護者として、アイルランドの首相、エンダケニーを効果的に使用しました[1418]。  
 フランスは、Google e50mがデータ同意ポリシーについて十分にユーザーに伝えなかったか、情報の使用方法を十分に制御できなかったことを認めました[1534]。  
26。  
2米国のプライバシー規制米国では、企業はほとんどの場合、政府にプライバシーを主に「自主規制」に委ねるよう説得することができました。  
 一般に、プライバシーに関する連邦政府の記録および通信は規制されていますが、ビジネスデータはほとんど制御されていません。  
 ほとんどの州には違反開示法もあります。この法律では、居住者の個人情報を危険にさらすセキュリティ上の失敗を確認し、それを通知する必要があります。  
CEOのレーダーにプライバシーをかけ始めた最初のケ​​ースは2006年に、ChoicepointがFTCが提起した訴訟を解決するために1,000万ドルを支払い、加入者を適切に審査し、詐欺師が16万人以上のアメリカ人の個人情報を購入することを許さなかったために発生しました。 「個人情報の盗難」800件[671]。  
700万件の顧客のクレジットカード情報が盗まれました[1159]。 2010年、アルバートゴンザレスはこのために懲役20年を過ごしました。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。  
セキュリティエンジニアリング861ロスアンダーソン26。  
 プライバシーとデータ保護20年の監査を条件とする[181]。  
 Cスイートの大虐殺が続いており、米国11と他の国12の両方で、サイバーセキュリティが企業の課題に着実に進んでいます。  
 これはプライバシー投票のイニシアチブに続き、それが投票所に行き渡された場合、さらに厳しいプライバシー法が定着しました。  
 大手テクノロジー企業の弁護は、投票法案の代わりに新しい法律を交渉することでした。そのため、彼らはそれを後で修正したり、連邦法で踏みにじったりすることができました。  
欧州の忘れられる権利は、米国のFirstAmendmentのおかげで重要ではありません。現在、非常に重要な政策問題は、この法律が他の州によって漸進的にコピーされているのか、それともビッグテックが管理しているのかということです13。  
26。  
3断片化？1998年以来、ヨーロッパの法律は、法律が同等の保護または他の保護手段を提供していない国の組織に企業が個人データを送信することを禁止しています-実際には、それはアメリカとインドを意味します。  
 2000年、欧州委員会は、これにより「十分な保護」が得られるとの効果を与える行政決定を採択しました。  
セーフハーバーを殺害した事件は、オーストリアの弁護士であるマックス・シュレムスがフェイスブックに対して提起した。  
 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年にシンガポールのIntegrated Health InformationSystemsのBruce Liang氏。また、VWのMartin WinterkornやAudiのRupertStadlerも数えることができます。彼らは、自動車の排気ガスをハッキングする会社を率いていました。  
セキュリティエンジニアリング862ロスアンダーソン26。  
 プライバシーとデータ保護は、NSAがスパイしている可能性があるとEU市民が訴えた場合に不平を述べることができる追加およびオンブズパーソンです[1474]。マックスもこれを2020年7月に正当に打ち倒したヨーロッパの法廷に持ち込みました[1683]。  
 裁判所はまた、プライバシー当局が苦情を受け取ったときに行動を起こす義務があると判決しました。  
米国でデータを処理する多くの企業は、その間に契約にフォールバックし、顧客が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よう顧客に強いました。  
 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、Snowdenの開示がこのアクセスの体系的な使用（およびEU法の観点からの乱用）を文書化する場合、米国の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。  
 より知識のある企業の一部は、最終的にはヨーロッパおよびヨーロッパの法律の下でヨーロッパのデータを処理する必要があると想定しています。マイクロソフトはドイツにデータセンターを数年間ドイツの管財人の管理下に置きましたが、その後気が変わりましたが、Googleはミュンヘンで数年間プライバシーの研究と開発を行ってきました。  
 ああ、20％が過去12か月間に何らかのオンライン詐欺に遭遇しました[144]。  
 たとえば、英国離脱国民投票の後、英国情報委員会は、CambridgeAnalyticaに世界中の8700万人の個人データを収集させた後、Facebookに500,00015ポンドを確定し、これを使用してBrexit国民投票と米国2016年大統領選挙の両方で選挙広告をターゲティングしました[957]。  
 これが同じように行われる場合、ECJの判決は、欧州評議会のメンバーであるが英国やロシアなどのEUのメンバーではない国に拡大されます。  
セキュリティエンジニアリング863ロスアンダーソン26。  
 情報の自由イノベーション。  
 Elec-tronic Privacy Information Center16は、Cambridge Analyticaのスキャンダルが破られて以来、FacebookがFTCとの2011年の和解条件に違反していると主張してきた。  
7情報の自由情報は弱いものから強力なものへと流れ、その力を高め、他の人が説明するのを難しくする傾向があります。  
知識は永遠に無知を支配します。そして、自分たちの総督になることを意味する人々は、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みられました：税申告書はアイスランドと一部のスイスのカントンで公開され、金持ちは低い宣言された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、データの取得、送信、および保存のコストが下がることで当局に普及した監視技術が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、例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る。  
 いずれにせよ、Freedomof Information Actsは、一般に、それを差し控える正当な理由がない限り、市民が州が保持する情報のコピーを要求することを許可し、市民と州の間の情報の流れが完全に一方向ではないことを保証します。多くのヨーロッパの国々には白紙の法律があり、それによってほとんどの刑事上の有罪判決は判決の厳しさに依存する一定期間後に抹消され、2019年にペンシルベニア州、ユタ州、カリフォルニア州がそれに倣った[607]。  
16完全な開示：私は彼らの諮問委員会のメンバーです。  
セキュリティエンジニアリング864ロスアンダーソン26。  
 概要これは、データ保護と情報の自由の間の境界の変化の一例です。  
 3つ目は、犯罪統計の公開です。住宅所有者は、近所の人々が非難されることに異議を唱えています。データが細かすぎると、個々の被害者が特定されるリスクがあるかもしれません。  
1つの推論セキュリティ。  
8SummaryPublicポリシーは、セキュリティエンジニアの作業とますます絡み合っています。  
インテリジェンスコレクションはまた、防御的なセキュリティとプライバシーの両方に矛盾しています。  
 おそらく分析が行われると、機関の能力に対するSnowdenの効果は（技術をより多くの、そしてよりインテリジェントに使用するようにすることを通じて）技術的に大きくなり、一方、ポリシーの効果は、より多くの人々にとってプライバシーをより顕著にする。  
 他の国々も訴訟を起こし始めている。  
 インターネットは依然として、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を難しくしていますが、10年前に私たちが抱いていた楽観論の多くは、アラブの春の失敗で消滅しました。  
 AOLがスカンソープに住むことを禁じてから25年が経過し、著作権、過激化、嫌がらせ、偽のニュースについて話しているかどうかにかかわらず、大規模なフィルタリングは依然として多くのポリシー問題を引き起こしています。  
 これは、コンピューターとセキュリティエンジニアリングの拡散につながっています865ロスアンダーソン26。  
 私たちのセキュリティ、私たちの自由、私たちの生活の質を侵食するネットワーク活用ツール。  
 オンラインの害を軽減しながら監視エコシステムを理解して押し戻すことは、直接でも、私たちの執筆や教育を通じてでも、公の生活に関わることができる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、そうするでしょう。  
研究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取り組んできました。そして、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？ （そして、おそらく第4版がある場合は、哲学者を追加します。  
 エンジニアは、Rなどの経験豊富な内部関係者が作成した資料から、主要な情報源を探す必要があります。  
 ジョーンズ[992]エドスノーデンによって漏らされた何千ものドキュメントに。  
傍受と暗号化ポリシーの歴史に関する優れた本があり、ポリシープロセスに長い間関わってきたホイットディエとスーザンランダウによる[558]。また、暗号化ポリシーに関するNRCの研究も影響力があった[1411]。  
輸出管理の歴史は、1970年代と80年代に米国のコンピューター、半導体、エネルギー技術を購入しようとしたソビエトの試み、およびそれらをブロックしてそれらを養う米国とフランスの諜報機関の取り組みと結びついています。セキュリティエンジニアリング866ロスアンダーソン26。  
 誤解を招く情報：この作業に関与したCIAの異端者であるガスワイスに関する回想録[723]を参照してください。  
コンピューターフォレンジックに関する標準的な作業は、Tony SammesとBrianJenkinson [1644]によるものですが、Privacy Internationalは携帯電話フォレンジック[1555]に関する調査を行っており、司法省の「コンピューターの検索と押収に関するガイドライン」にも注目しています[550]。  
 コモンローの国でのコンピュータ証拠に関する標準的な作業は、StephenMason [1236]によるものです。  
 最近の資料は、EPIC [631]、EFF [618]、FIPR [708]、EDRi [643]、およびMax Schrems [1683]などの組織のWebサイトにあります。最後に、ケンブリッジアナリティカスキャンダルの決定的な物語は、内部告発者のクリスワイリー[2052]と、彼と他の人々が提供した情報[363]に基づくCaroleCadwalladrのジャーナリズムで本に語られています。