대화 재구성하기: 암호화 논쟁에 대한 심층 분석

정부는 암호화가 법 집행 기관의 업무 수행을 방해한다고 말하지만, 암호화 기술은 어린이와 기타 취약 계층을 포함한 모든 사람을 보호합니다.

2024년 2월

편집자:

Heather West | 수석 이사
+1 202.344.4597
HEWest@Venable.com

Zack Martin | 수석 정책 고문
+1 202.344.4393
ZPMartin@Venable.com

Ivy Orecchio | 프로젝트 매니저
+1 202.344.4277
IDOrecchio@Venable.com

CENTER FOR CYBERSECURITY POLICY AND LAW

목차

경영진 요약

암호화는 온라인 커뮤니케이션을 보호하고, 언론의 자유를 실현하며, 금융 거래를 보호하는 등 데이터 프라이버시 및 보안에 중요한 역할을 합니다. 사이버보안 정책 및 법률 센터는 대다수의 사이버보안 커뮤니티와 함께 암호화 약화가 모든 조직과 개인의 보안, 개인정보 보호, 시민의 자유, 중요한 사회적 이익을 위태롭게 할 것이라고 믿습니다.

암호화는 신원 도용이나 불법 감시와 같은 범죄로부터 개인을 보호하지만, 법 집행 기관과 국가 보안 기관은 암호화로 인해 법 집행 기관이 범죄와 공공 안전 위협을 조사하기가 더 어려워지거나 불가능해진다고 주장합니다. 일부에서는 디지털 시대에는 공공 안전, 테러, 아동 성 학대 자료(CSAM)와 관련된 통신을 감청하고 해독하는 등 디지털 증거가 수사에 반드시 필요하다고 주장합니다.

암호화에 반대하는 사람들은 이 문제를 양측이 대립하는 논쟁으로 몰아가지만, 사실 우리는 같은 적에 맞서 공동의 대의를 위해 단결하고 있습니다. 암호화는 어린이와 기타 취약 계층을 포함한 모든 사람을 보호합니다.
소셜 미디어 사이트와 메시징 애플리케이션을 포함한 기술 기업은 범죄 활동의 통로가 되거나 플랫폼에 불법적인 자료를 보유하는 것을 원하지 않습니다.

이 백서의 저자들은 이제 이러한 논의를 재고해야 할 때라고 생각합니다. 따라서 정부와 법 집행 기관은 암호화를 우회할 수 있는 유비쿼터스 감시를 의무화하기보다는 법 집행 및 온라인 보안에 영향을 미치는 정책과 법률에 대해 실용적이고 점진적인 접근 방식을 취해야 합니다.

이 백서에서 확인할 수 있습니다:

- 암호화 정책에 대한 역사적인 논의와 논쟁을 살펴보세요;
- 현재 정책 및 법률의 맥락에서 제안서 중 반복되는 주제를 검토하세요;
- 현대의 암호화 논의가 어떻게 진행되어야 하는지 정립합니다.
- 담론이 변경되지 않은 채로 유지될 경우 발생할 수 있는 문제를 해결하세요.

사이버 보안 및 법률 센터 소개

사이버보안 정책 및 법률 센터는 정부, 민간 업계, 시민 사회에 보안 위협을 더 잘 관리할 수 있는 사례와 정책을 제공하여 전 세계 사이버 보안을 강화하는 데 전념하는 독립 기관입니다.

2017년 Venable LLP의 사이버보안 서비스 그룹 내 501(c)(6) 비영리단체로 설립된 이 센터는 정책 전문성과 글로벌, 국가, 지역 차원의 소집력을 결합하여 업계 리더와 정책 입안자가 함께 연합을 구성하고 실제 성과를 창출하는 이니셔티브를 시작합니다. 합의 중심의 위험 관리 기반 접근 방식을 적용하는 이 센터는 디지털 인프라와 정보 시스템 보안의 최전선에 있는 사람들의 관점과 관행에서 도출된 실용적인 솔루션과 정책 권장 사항을 홍보함으로써 사이버 보안에 대한 복잡성을 해소하고 혼란을 없애고자 노력합니다.

소개

기술은 우리의 일상에 깊숙이 자리 잡고 있습니다. 인터넷은 말 그대로 우리 손끝에 있고, 회전식 전화기는 FaceTime 통화와 Zoom 회의를 가능하게 했으며, 편지는 문자 메시지와 이메일로 바뀌었고, 웨어러블 기기는 심박수, 혈당 수치 및 기타 건강 지표를 추적하여 건강에 대한 실시간 통찰력을 제공합니다. 통신 기술과 사물 인터넷은 우리의 현실을 확장하고 전 세계 어디에 있든 친구, 가족, 커뮤니티와 연결 상태를 유지할 수 있게 해줍니다. 이러한 디지털 기술의 사용이 확대됨에 따라 기업들은 데이터 보호를 위해 암호화를 사용하는 등 보안 유지에 힘쓰고 있습니다.

디지털 환경의 눈부신 발전과 함께 범죄자와 악의적인 행위자들도 이러한 기술을 이용하고 있습니다. 법 집행 기관과 국가 보안 기관 등 사회를 보호해야 하는 기관들은 수십 년 동안 이러한 기술의 보안 및 암호화 메커니즘으로 인해 업무를 제대로 수행하지 못하고 있다고 우려하며 기술 기업에 책임을 돌리고 있습니다.

개인 정보 보호와 보안은 Facebook 기술에 내장되어 있으며, 점점 더 당연한 것으로 받아들여지고 있습니다. 암호화는 중요한 개인 데이터 보호의 핵심입니다. 법 집행 기관의 제안은 간단합니다. 암호화된 자료에 대한 액세스 권한을 부여하고 메시지를 스캔하여 유해한 자료를 식별할 수 있는 시스템을 구축하는 것입니다. 관계자들은 이 제안이 어린이를 보호하고, 불법 약물이 유통되지 않도록 하며, 부패를 방지하고, 잠재적으로 폭력 범죄를 막는 데 도움이 될 것이라고 말합니다. 그러나 이러한 지나치게 단순화된 솔루션은 사생활을 침해하고 개인을 악의적인 행위자나 도청자에게 노출시킬 수 있는 매우 위험할 수 있습니다. 그럼에도 불구하고 법 집행기관과 정책 입안자들은 플랫폼이 엔드투엔드 메시징 암호화를 추가하고 디바이스의 데이터를 암호화하는 방향으로 나아감에 따라 계속해서 예외를 모색하고 있지만, 이러한 제안은 모든 사람의 디지털 생활을 안전하게 지키는 데 있어 암호화가 갖는 중요한 역할을 적절히 설명하지 못하고 있습니다.

암호화는 정보 보안을 유지하는 데 매우 중요합니다. 기업들은 지난 50년 동안 암호화를 사용하여 데이터를 침해로부터 보호하고 커뮤니케이션과 운영을 보호해 왔으며, 의료, 금융 서비스, 교육 등 많은 분야에서 법이나 모범 사례 및 표준을 통해 데이터를 암호화해야 하는 업계 요구 사항이 있습니다. 법 집행기관, 군대, 정부 관계자들도 암호화의 중요성에 동의하며 자체 시스템과 데이터를 보호하기 위해 동일한 도구와 기술을 사용하고 있습니다. 그러나 이러한 공공 기관 중 상당수는 어린이와 공공 안전을 보호한다는 명목으로 암호화를 우회하는 방법을 원합니다. 안타깝게도 한 기관의 암호화가 깨지면 보호하고자 하는 개인을 포함한 모든 기관의 암호화가 깨질 수 있습니다.

'암호화 논쟁' 또는 '암호화 전쟁'을 반대 세력의 충돌로 규정하는 것은 그 핵심에 있는 공동의 목표와 상호 이익에 해를 끼칩니다. 이 논쟁의 핵심 쟁점, 특히 아동 성학대 및 아동 성착취물(CSAM)과의 싸움과 대테러 노력은 기술 발전과 무관하게 지속되고 있습니다. 범죄 활동은 인터넷과 암호화 이전부터 존재했던 새로운 일이 아닙니다. 소셜 미디어 플랫폼과 메시징 애플리케이션을 운영하는 기술 기업들은 이러한 자료가 자사 플랫폼에 게시되는 것을 원치 않으며, 이를 방지하기 위해 상당한 자원을 투입하고 있습니다.[1] 표면적으로 반대되는 양상을 보이는 이 둘을 하나로 묶는 공통의 대의는 아동과 대중을 보호하기 위해 이러한 범죄를 처음부터 예방해야 한다는 점입니다.

이러한 공동의 노력에도 불구하고 공동의 해결책을 향한 의미 있는 진전은 여전히 요원합니다. 이러한 문제를 사회에서 근절할 수 있는 만능 해결책, 은총, 요술 지팡이는 없으며 경우에 따라서는 제안된 해결책이 매우 위험한 양날의 검이 될 수 있다는 점을 인식하는 것이 필수적입니다.

예를 들어, 최근의 한 캠페인은 온라인 클라우드 스토리지 플랫폼인 iCloud에서 아동 성학대물을 탐지하기 위한 Apple의 노력을 구체적으로 보여줍니다. 이 빌보드 광고에는 인공지능이 생성한 얼굴이 위장한 아동의 이미지와 함께 "아동 성적 학대가 iCloud에 저장되어 있습니다. Apple은 이를 허용합니다."라는 문구가 등장합니다. 이는 애플이 종단 간 암호화 여부와 관계없이 iCloud에 저장된 이미지를 스캔하여 CSAM을 찾는 개인정보 및 보안 보호 시스템 개발을 중단하기로 한 결정에 따른 것이지만, 이는 사실과 다릅니다.[2] 애플은 수년간의 연구 끝에 "모든 사용자의 비공개 저장 iCloud

[1] https://www.thorn.org/blog/new-report-shows-an-increased-effort-by-tech-companies-to-detect-csam-on-the-internet/

[2] "Apple's Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy," https://www.wired.com/story/apple-csam-scanning-heat- initiative-letter/

데이터를 캔에 담는다면 데이터 도둑이 찾아서 악용할 새로운 위협 벡터를 만들 수 있다는 결론을 내렸습니다. 또한 의도하지 않은 결과를 초래할 수 있는 미끄러운 경사면을 만들 수도 있습니다. 예를 들어 한 가지 유형의 콘텐츠를 검색하면 대량 감시에 대한 문이 열리고 콘텐츠 유형 전반에 걸쳐 다른 암호화된 메시징 시스템을 검색하려는 욕구가 생길 수 있습니다."[3]

따라서 암호화에 대한 논쟁은 복잡하고 어려운 문제들로 가득 차 있으며, 양측 모두 간단한 해결책을 찾고 있습니다. 사이버보안 정책 및 법률 센터는 어린이와 대중의 안전이 가장 중요하지만, 다른 모든 공공 및 민간 부문 조직과 개인의 개인정보와 보안을 위협하지 않으면서도 범죄에 효과적으로 대처할 수 있는 방법이 있다고 믿습니다. 그럼에도 불구하고 완벽한 것이 진보의 적이 되어서는 안 됩니다. 잠재적인 해결책을 논의하는 동안 개인정보 보호와 보안을 강화하고 커뮤니티를 보호할 수 있는 점진적인 조치를 놓치지 말아야 합니다. 암호화 미봉책은 기술적, 정책적 난제로 가득 차 있어 안전하게 배포하는 것이 불가능하지는 않더라도 어렵게 만들 수 있습니다. 하지만 전체 디지털 생태계와 이를 사용하는 모든 사람을 보호하는 보안을 훼손하지 않으면서도 대중과 어린이의 안전을 보호할 수 있는 방법이 있다고 굳게 믿습니다.

암호화를 둘러싼 역사적인 논쟁

1992년 로버트 레드포드와 시드니 포이티에 주연의 영화 '*스니커즈*에서 한 암호학자가 어떤 암호화 체계도 뚫고 보이지 않는 모든 것을 해독할 수 있는 장치를 만들었습니다. 정부 해킹 사건으로 법을 어긴 후 새로운 신분을 갖게 된 로버트 레드포드와 그의 팀은 이 장치로 연결되는 일자리에 고용된 후 윤리적 딜레마에 직면하게 됩니다. 전 세계 모든 시스템의 정보에 액세스할 수 있는 권한이 그들의 손끝에 있지만 너무 과한 것일까요? 결국 레드포드의 팀은 그렇다고 판단하고 장치를 파괴하여 악당과 이를 노리는 법 집행 기관을 모두 물리쳤습니다.

이 영화는 30년 넘게 관객을 즐겁게 해왔지만, 암호는 외교, 첩보 활동, 전쟁 수행에 사용되어 왔기 때문에 그 핵심에 있는 수수께끼는 수세기 동안 논쟁의 대상이 되어 왔습니다. 역사를 통틀어 비밀 코드와 암호의 사용은 안전한 통신을 유지하고 민감한 정보를 보존하는 데 필수적인 요소였습니다. 전쟁에서 승리하고 패배했으며 범죄를 예방했습니다. 그러나 이러한 암호의 사용은 잠재적인 위협이나 공격자가 불법 활동에 동일한 도구와 기술을 악용하는 것을 방지해야 할 필요성을 강조합니다.

---

[3] Ibid

현대의 디지털 암호화에 대한 논쟁은 공용 인터넷이 등장하기 이전부터 있었고 냉전 시대에도 중요한 역할을 했습니다. 제2차 세계대전 이후 미국은 통신용 암호화 기술에 대한 수출 통제를 시행하여 강력한 암호화 기술의 수출을 금지했습니다. 미국과 마찬가지로 많은 유럽 국가들도 처음에는 강력한 암호화 기술을 군수품 또는 군사적 용도로 사용될 수 있는 이중 용도 품목으로 간주하여 엄격한 수출 통제를 시행했습니다.[4] 이는 어느 정도 성공을 거두었지만 일반적으로 미국을 포함한 전 세계에서 약한 암호화를 사용하는 결과를 낳았습니다.[5]

1990년대에 암호화에 대한 논의가 발전했습니다. 상업용 인터넷이 시작되고 특히 금융 거래에 개인용 컴퓨터가 널리 사용되면서 암호화는 더욱 주류가 되었습니다. FBI와 NSA(국가안보국)는 통신에서 종단 간 암호화를 사용하는 것에 대해 공개적으로 반대하기 시작했습니다.[6] 1993년, 클리퍼 칩이라고 불리는 암호화된 통신에 접근할 수 있는 칩을 개발했습니다.[7] 이 칩은 제3자(이 경우 정부)가 암호화된 콘텐츠를 읽기 위해 암호 해독 키에 액세스할 수 있도록 하는 개념인 키 에스크로를 사용했습니다. 결국, 시민 자유와 개인정보 보호 옹호자들의 분노와 함께 부실하고 안전하지 못한 설계가 결국 승리했고, 오늘날의 휴대폰에는 법 집행 기관이 대화를 엿들을 수 있는 칩이 없습니다.

1996년 39개국이 이중용도 기술을 포함한 수출 통제에 관한 바세나르 협정에 서명하면서 보안 수준이 낮은 형태의 암호화는 더 이상 수출 통제를 받지 않게 되었습니다.[8] 미국에서는 암호화를 통한 안보와 자유(SAFE) 법이 냉전 시대의 정책으로 인해 발생한 문제를 해결하기 위해 노력했습니다. 수십 년 동안 강력한 암호화 제품은 엄격하게 규제되어 해외에서 판매되지 못하거나 약한 '수출 등급' 버전으로 수출해야 했습니다. 초당적인 법안은 국가 안보와 기술 발전 및 개인의 권리 사이의 균형을 맞출 필요성을 강조했습니다. 소프트웨어 기업들은 기존의 수출 통제가 혁신을 저해하고, 수십 년 된 정책이

---

[4] Ihttps://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220, https://www.sciencedirect.com/science/article/abs/pii/B9780444516084500274?via%3Dihub

[5] "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8

[6] "The state of encryption: How the debate has shifted," https://opensource.com/article/18/6/listening -susan-landau

[7] "The Short Life and Humiliating Death of the Clipper Chip," https://gizmodo.com/life -and-death-of-clipper-chip-encryption-backdoors-att- 1850177832

[8] https://www.armscontrol.org/factsheets/wassenaar

비효율적이며 미국 경제에 부정적인 영향을 미쳤다는 증거가 있다고 주장했습니다.[9] SAFE 법안이 법으로 통과되지는 않았지만 1999년 가을, 클린턴 행정부는 소매 암호화 제품의 수출에 대한 제한을 없애는 등 법안의 거의 모든 조항을 시행하는 정책을 채택했습니다.[10]

이러한 글로벌 정책 변화에 대응하기 위해 NSA는 강력한 암호화의 기반이 되는 암호화 표준을 약화시키고 대중의 감시를 받지 않는 백도어를 만들기 위해 비밀리에 작업을 시작했습니다.[11] 2006년까지 NSA는 세 개의 항공사, 여행 예약 시스템, 외국 정부의 원자력 부서 등의 통신에 액세스했습니다.

가상 사설망을 크래킹하여 정부의 인터넷 서비스를 해킹했습니다. 이는 2013년 스노든 폭로를 통해 밝혀졌는데, 이 폭로에서는 스파이 기관이 암호화 키를 생성하는 데 사용되는 난수 생성기를 손상시켜 암호화된 통신에 액세스하는 방법을 기록했습니다.[12]

매사추세츠 공과대학(MIT)의 2015년 기술 보고서는 2000년대 초반에도 암호화된 콘텐츠에 대한 이러한 액세스를 허용하는 것은 문제가 있었으며 인터넷의 발전과 중요성 증가로 인해 오늘날에는 훨씬 더 심각해질 것이라고 밝혔습니다.[13] "수백만 개의 앱과 전 세계적으로 연결된 서비스가 있는 오늘날 인터넷 환경의 복잡성으로 인해 새로운 법 집행 요건으로 인해 예상하지 못한, 탐지하기 어려운 보안 결함이 발생할 수 있습니다"라고 보고서는 명시하고 있습니다. "이러한 기술적 취약점 외에도 전 세계적으로 예외적인 액세스 시스템이 배포될 것이라는 전망은 이러한 환경을 어떻게 관리하고 그러한 시스템이 인권과 법치를 존중할 수 있도록 보장하는 방법에 대한 어려운 문제를 제기합니다."

NSA가 정보에 액세스하기 위한 수단으로 네트워크 취약점을 악용하는 동안, FBI는 암호화에 대한 다음 싸움에서 선두를 유지했습니다. 2015년, 영국과 미국의 정치 및 법 집행 기관 지도자들은 암호화가 법

9 https://slate.com/technology/2015/06/safe-act-the-right-to-strong-encryption-almost-became-law-in-the-90s.html

10 https://www.govinfo.gov/content/pkg/WCPD-1996-11-18/pdf/WCPD-1996-11-18-Pg2399.pdf

11 https://www.brookings.edu/articles/a-brief-history-of-u-s-encryption-policy/

12 https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2&_r=2

13 "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf?sequence=8

집행 기관의 범죄 수사 능력을 위협한다며 다시 한 번 암호화에 반대하는 목소리를 냈습니다.[14]

이 논쟁은 캘리포니아 샌버나디노에서 발생한 총기 난사 사건 이후 다시 수면 위로 떠올랐습니다. FBI는 추가 단서를 추적하기 위해 법원에 범인의 아이폰에 있는 비밀번호(기기 암호 해독)를 해독해달라고 요청했지만 애플은 이를 거부했습니다.[15] 결국 FBI는 기기 해킹이 가능한 제3자 업체를 찾았지만 메시지와 기기에 대한 정부 백도어 문제가 다시 한 번 제기되었습니다. 당시 법안이 제안되었지만 진전된 것은 없었습니다. 이 사건은 Apple에 기기 암호 해독을 강요한 가장 주목받는 사건이었지만 유일한 사건은 아니었습니다.[16], [17] Apple에 의해 최소 5번의 시도가 있었지만 모두 무산되었습니다. FBI가 기기에 액세스했지만 새로운 정보를 찾지 못했습니다.[18]

반복되는 주제와 현행 정책 및 법률

암호화 논쟁을 통해 암호화 알고리즘과 암호화된 콘텐츠에 대한 백도어와 프런트도어, 강력한 암호화 사용의 불법화 등 여러 가지 제안이 등장했습니다.

제안서	도전 과제
중개 액세스(키 에스크로): 신뢰할 수 있는 제3자가 암호화 키를 보관하여 특정 조건이 충족될 때 법 집행 기관이 암호화된 데이터에 액세스할 수 있도록 하는 방식입니다.	제3자의 보안 및 신뢰성으로 인해 불필요한 위험(예: 오용, 무단 액세스)이 발생할 수 있습니다. 키 보유자를 표적으로 삼으면 치명적인 공격이 발생할 수 있습니다. 키를 재조립하거나 전송해야 하는 경우 데이터에 빠르게 액세스하기가 어렵습니다.
중개되지 않은 액세스: 법 집행 기관이 데이터 소유자나 처리자의 개입 없이 암호화된 데이터에 액세스하기 위해 도구와 기술을 배포하는 것을 말합니다.	법 집행 기관에서 사용하는 백도어는 악의적인 공격자에 의해 악용되거나 무단 사용에 악용될 수 있습니다. 데이터 주체가 알지 못하거나 동의하지 않은 상태에서 데이터에 액세스하는 것은 다양한 개인정보 보호, 시민권 또는 시민 자유 문제를 야기할 수 있습니다.

[14] Ibid

[15] A Year After San Bernardino And Apple-FBI, Where Are We On Encryption?" https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption

[16] https://www.justsecurity.org/wp-content/uploads/2016/03/Apple-All-Writs-Apple-Requests-Received-Letter.pdf

[17] https://www.theguardian.com/technology/2016/feb/23/apple-new-iphone-models-san-bernardino-shooter-all-writs-act-department-of-justice

[18] https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads

기술 지원: 기술 회사가 암호화를 약화하거나 데이터를 해독하는 도구를 만들어 법 집행 기관이 암호화된 데이터에 액세스할 수 있도록 도와야 할 수 있는 프로세스입니다.	도구나 백도어를 만들면 시스템이 약해져 공격에 더 취약해집니다. 기술 기업이 자사의 제품이 법 집행을 위해 의도적으로 약화되었다고 생각되면 사용자의 신뢰를 잃을 수 있습니다. 기술 기업은 규정 준수 요구 사항을 예상하여 기본적으로 더 약한 시스템을 구축할 수 있습니다.

지난 몇 년 동안의 제안으로 법 집행 기관과 정부가 이러한 암호화 공격에 대응하는 방식이 바뀌었지만, 잠재적인 영향력에는 변화가 없었습니다.

영국의 온라인 안전법

2023년 9월, 영국은 웹사이트 및 기타 인터넷 기반 서비스에 불법적이고 유해한 콘텐츠가 없도록 하기 위한 온라인 안전법[19]을 통과시켰습니다. 이 법은 검색 엔진, 소셜 미디어 플랫폼, 사용자 제작 콘텐츠 호스트, 온라인 포럼, 게임, 음란물 사이트 등 광범위한 온라인 서비스 제공업체에 적용됩니다.[20]

이 법안은 종단 간 암호화를 명시적으로 금지하지는 않지만, 정부가 승인한 기술을 사용하여 콘텐츠 필터링과 연령 확인을 의무화합니다. 이 법안에는 종단 간 암호화 메시지를 제공하는 기술 기업이 메시지 콘텐츠를 스캔하여 당국에 보고하도록 강제하는 조항도 포함되어 있습니다.[21] 기술 기업의 강력한 반대에 부딪혔지만, 통과된 법에 포함된 추가 수정안에 따르면 기업은 "기술적으로 실현 가능하고 기술이 다음을 충족하는 것으로 인증된 경우"까지 암호화된 메시지를 스캔할 필요가 없다고 명시되어 있습니다.[22]

아동 성 학대 및 착취 콘텐츠만 탐지할 수 있는 최소한의 정확도 기준입니다." 그러나 암호화 정책의 역사를 보면 법 집행 기관, 기술 회사, 기술자 간에 기술적으로 실현 가능한 부분에 대해 의견이 크게 엇갈리고 있음을 알 수 있습니다.

인기 메시징 앱인 Signal은 암호화 백도어가 요구될 경우 영국 시장에서의 운영을 중단하겠다고

[19] https://bills.parliament.uk/bills/3137

[20] "UK's controversial online safety bill set to become law," https://www.computerworld.com/article/3706810/uks-controversial-online-safety-bill- set-to-become-law.html

[21] https://www.gov.uk/government/publications/end-to-end-encryption-and-child-safety/end-to-end-encryption-and-child-safety

[22] https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email

밝혔습니다.[23] 영국 내무부도 페이스북과 인스타그램에 엔드투엔드 암호화를 도입하는 Meta에 반대하는 캠페인을 시작했으며, 그래픽 언어를 사용하여 탐지되지 않을 수 있다고 생각하는 CSAM을 설명했습니다. 한 동영상에는 아동 성 학대 피해자가 마크 저커버그 메타 대표에게 직접 암호화 도입 계획을 재고해 달라고 호소하는 내용이 담겨 있습니다.[24] 온라인 안전법이 통과된 후 영국 내무부의 압력에도 불구하고[25] 메타는 오랫동안 계획했던 메신저용 엔드투엔드 암호화를 올해 말까지 암호화된 WhatsApp 제품에 도입하고,[26] 플랫폼에서 모든 메시지를 엿볼 필요가 없는 방법을 사용하여 그루밍 및 아동 학대 콘텐츠 공유를 지속적으로 모니터링할 계획입니다.[27]

호주의 지원 및 접근법

법안을 통해 암호화 사용을 억제하려는 시도는 영국만이 아닙니다. 호주는 2018년 법 집행 기관과 정보 기관이 디지털 시대에 효과적으로 활동하고 테러와 범죄를 해결하는 데 필요한 도구를 갖추기 위해 지원 및 접근법을 통과시켰지만,[28] 이는 암호화에 대한 공격으로 널리 묘사되었습니다.[29]

이 법은 장비 제조, 소프트웨어 개발 또는 업데이트, 웹사이트 운영에 관여하는 통신 서비스 제공업체, 기업 또는 개인이 법 집행 및 보안 기관과 협력해야 할 책임을 강화했습니다. 또한 법 집행 기관을 위한 컴퓨터 접근 영장을 신설하고 보안 기관이 수색 영장을 통해 계정 기반 데이터와 컴퓨터 및 모바일 디바이스의 암호화되지 않은 데이터에 접근할 수 있는 수색 및 압수 권한을 강화했습니다.[30]

이 법의 주요 메커니즘에는 데이터에 대한 예외적 접근에 대한 자발적 및 강제적 요청과 함께 조직이 자체 암호화 해제, 암호화 다운그레이드, 백도어 구축 등 새로운 기능 구축을 포함한 지원을

---

[23] https://twitter.com/mer____edith/status/1704477739871273397

[24] https://subscriber.politicopro.com/article/2023/09/u-k-dials-up-fight-with-meta-over-encryption-00117008?source=email

[25] https://www.reuters.com/technology/uk-urges-meta-not-roll-out-end-to-end-encryption-messenger-instagram-2023-09-19/

[26] https://about.fb.com/news/2023/12/default-end-to-end-encryption-on-messenger/

[27] https://www.theguardian.com/technology/2023/jun/07/meta-instagram-self-generated-child-sexual-abuse-materials

[28] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[29] https://www.eff.org/deeplinks/2018/12/new-fight-online-privacy-and-security-australia-falls-what-happens-next

[30] https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/

제공하도록 요구하는 조항이 포함되어 있습니다.[31]

이 법은 통과 속도, 투명성 부족, 부실한 협의 절차에 대해 기술 기업, 개인정보 보호 옹호자, 일반 대중으로부터 지속적인 비판을 받아왔습니다. 법에 내장된 안전장치가 업계에 암호화를 깨도록 요구할 수 없다고 주장하지만, 비평가들은 기업이 새로운 액세스 기능을 만들도록 강제하는 법의 기능이 기업이 암호화를 약화하거나 백도어를 구축하도록 강요하는 데 사용될 수 있다고 주장합니다. 이 법은 호주인의 정보 보안을 침해함으로써 전 세계 기업과 사람들의 정보를 위험에 빠뜨리는 등 광범위한 영향을 미칠 수 있습니다.

2020년 6월 현재, 강제 명령이 발령되지 않았고 지원 요청 초안이 작성된 건수는 20건 미만입니다.[32]

기타 제안

전 세계 각국 정부는 암호화에 대해 다양한 접근 방식을 취하고 있습니다. 아래는 전 세계에서 제안되고 통과된 정책 및 법률의 요약과 잠재적 시사점을 담은 표입니다.

국가	법률	요약	암호화 시사점
인도	2000년 정보 기술법 제69A조(통과)	이 법에 따라 인도 정부는 인터넷 서비스 제공업체(ISP)와 통신 서비스 제공업체를 포함한 온라인 중개자에게 국가 안보에 위협이 된다고 판단되는 콘텐츠나 정보를 차단하도록 지시할 수 있는 권한을 갖고 있습니다.[33]	올해 초 인도 정부는 이 법령을 활용하여 테러리스트들의 통신을 돕는다는 이유로 14개의 암호화된 메시징 앱을 금지하고 전국적으로 접속을 차단했습니다.

[31] https://www.abc.net.au/news/2018-12-04/encryption-whatsapp-signal-messages-explained/10580208

[32] https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees/commjnt/30904d8b-7cfb-4ef0-99fb- fba2299b57bf/&sid=0000

[33] https://tutanota.com/blog/posts/apps-banned-india

유럽 연합	아동 성학대 예방 및 퇴치를 위한 규정(아동 성학대 규정 또는 CSAR)(안)	이 제안은 처음에 서비스 제공업체가 서비스에서 CSAM을 탐지, 신고 및 제거하도록 요구했습니다. 이 규칙에 따르면 서비스 제공업체는 암호화 메시지를 포함하여 서비스에서 CSAM 및 아동 그루밍을 사전에 검사해야 합니다.[34] 유럽 의회의 시민 자유, 법무 및 내무 위원회(LIBE)는 이 조항을 삭제하고 표적 감시만 허용하기로 의결했습니다.[35]	유럽 의회에서 실시한 영향 평가에 따르면 초기 제안은 종단 간 암호화와 디지털 통신의 보안을 약화시킬 수 있으며 모든 통신 메타데이터를 검사하는 것은 비례하지도 않고 필요하지도 않다는 유럽사법재판소의 판례에 위배될 가능성이 있다고 결론지었습니다.[36] 이후 의회는 다음을 제외한 문안을 채택했습니다. 종단 간 암호화를 탐지 명령의 범위에서 제외하고, 다른 완화 조치가 효과가 없는 경우에만 사용해야 하며, 최종 본문에서는 표적 감시만 허용한다는 점을 명확히 했습니다.[37]

영국	수사권 조정법(IPA) 개정 사항	IPA는 특별 액세스와 관련하여 광범위한 요구 사항을 적용하고 있으며, 이번 업데이트에는 글로벌 시장에 영향을 미칠 수 있는 새로운 보안 기술을 사전 승인하거나 차단하는 기능이 포함되어 있습니다.[38]	기존 IPA에 따르면 영국 정부는 모든 사용자의 서비스를 약화, 제한 또는 백도어 암호화를 포함하여 변경할 수 있는 것으로 보입니다. 또한 기업은 종단 간 암호화와 같은 보안 기능 도입을 포함하여 조사에 영향을 미칠 수 있는 방식으로 서비스를 변경하기 전에 정부에 통보해야 합니다.[39]

[34] https://cyberlaw.stanford.edu/blog/2023/06/eu-member-states-still-cannot-agree-about-end-end-encryption

[35] https://edri.org/our-work/csar-european-parliament-rejects-mass-scanning-of-private-messages/

[36] European Parliament. (2023, April). Complementary impact assessment - Proposal for a regulation laying down the rules to prevent and combat child sexual abuse. https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf

[37] https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass- surveillance

[38] https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-factsheets/investigatory-powers-amendment-bill- overview#what-does-the-investigatory-powers-amendment-bill-do

[39] https://www.justsecurity.org/87615/changes-to-uk-surveillance-regime-may-violate-international-law/

미국	인터랙티브 기술 악용 및 만연한 방치 근절법(EARN IT 법)	이 법안은 국가 온라인 아동 성착취 방지 위원회를 설립하고, 통신 품위법 230조를 개정하여 서비스 제공자에 대한 보호 조항을 삭제하고, 기존 아동 성착취 관련 법령의 집행을 강화함으로써 아동 성착취 문제를 해결하는 것을 목표로 합니다.[40]	EARN IT 법은 서비스 제공업체가 엔드투엔드 암호화를 제거하거나 백도어를 만들도록 장려하여 어린이 및 기타 취약 계층을 포함한 모든 사용자에게 취약성을 초래합니다. 또한, 위원회가 개발할 모범 사례는 의회 지도부가 제안한 위원의 과반수를 임명하는 등 정치적으로 주도될 수 있습니다.

최신 암호화 논쟁의 해법 찾기

카네기 국제평화재단, 프린스턴 대학교, 국제기술정책센터는 *새로운* 접근법을 찾기 위해 암호화 워킹그룹을 구성하여 암호화 논의를 면밀히 검토하고 있습니다. 이들은 2019년에 "암호화 정책 논의의 진전"이라는 보고서를 발표했습니다.[41] 이 그룹은 암호화된 데이터에 대한 법 집행 기관의 접근을 둘러싼 교착 상태를 해결하기 위해 제안된 접근 방식의 장점과 위험을 모두 포함하여 암호화의 사회적 영향을 평가하는 보다 유익한 방법을 제안합니다. 이 백서에서는 특히 휴대폰 암호화에 대해 자세히 살펴보고 법 집행기관의 접근에 초점을 맞춘 제안을 평가하기 위한 보다 구체적인 접근 방식을 자세히 설명합니다.

카네기 백서는 이 주제를 공정하고 다양한 이해관계자의 시각에서 바라보며 암호화에 대한 찬성과 반대라는 두 가지 주요 논거를 거부하는 것으로 시작합니다:

1. 법 집행 기관은 암호화된 정보에 액세스할 수 있는 방법을 모색하는 것을 중단해야 합니다.
2. 법 집행 기관은 합법적인 절차를 통해 모든 암호화된 데이터에 액세스할 수 없다면 대중을 보호할 수 없습니다.

궁극적으로 이 그룹은 추가 작업이 필요하며 휴대폰 암호화 사용 사례에서 진전이 이루어질 수 있다는 결론을 내렸습니다. 주요 내용은 다음과 같습니다:

- 휴대폰의 저장된 암호화 데이터에 대한 논의는 다양한 이해관계 커뮤니티에서 토론을 활성화하고 위험과 이점을 보다 명확하게 파악할 수 있게 해줄 것입니다.
- 이 분야의 기존 제안이 실행 가능하거나 향후 제안이 실행 가능하다는 징후가 없거나

[40] https://tutanota.com/blog/posts/earn-it-barr-encryption

[41] https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

현재로서는 정책 변경이 바람직하다는 징후가 없습니다.

- 이 주제에 대해 양측의 선의의 논쟁이 없다면, 이 중요한 암호화 논쟁에 대해 다른 곳에서도 선의의 논쟁이 없을 것입니다.

중요한 첫 번째 단계는 공통점을 파악하는 것입니다. 이 논의에는 우리 모두가 동의할 수 있는 요소들이 있습니다.

암호화는 대부분의 조직이 데이터를 보호하고 사용자가 본인임을 증명할 수 있는 최선의 방어책입니다. *주민등록번호*, 결제 카드 정보, 기타 개인 정보가 유출되는 대규모 데이터 유출 사고가 발생했고 앞으로도 계속 발생할 것이지만 암호화는 정보를 보호하는 최선의 수단입니다.[42] 반대로 범죄자가 키 저장소가 있거나 암호화 알고리즘에 잠금 해제 가능한 문이 있다는 것을 알고 있다면 이는 범죄자들에게 매우 매력적인 허니팟이 될 것이며, 이들은 자신의 목적을 위해 최선을 다해 잠금을 해제하려고 할 것입니다.

점진적인 변화가 앞으로 나아가기 위한 열쇠가 될 것입니다. 이전의 논쟁은 지나치게 단순화된 솔루션이 특징이었습니다. 현대의 암호화 논쟁은 기술의 급속한 발전으로 인해 이러한 시스템 내에서 복잡성과 상호운용성을 해결하는 것이 어떻게 변화하는 목표가 될 것인지 인식해야 합니다. "광범위한 예외적 액세스를 달성하려면 말 그대로 전 세계 수십만 명의 개발자와 함께 새로운 기술 기능을 배포하고 테스트해야 합니다."라고 MIT 보고서는 말합니다. "이는 유사한 기술을 사용하는 경향이 있고 새로운 기능으로 인해 발생할 수 있는 취약성을 관리할 수 있는 리소스가 있는 통신 및 인터넷 액세스 서비스에 현재 배포된 전자 감시보다 훨씬 더 복잡한 환경입니다." 암호화를 사용하고 콘텐츠를 전송하거나 저장하는 제품과 서비스의 수가 급증하면서 예외적인 액세스 문제의 복잡성이 증가했습니다.

'내 적의 적은 내 친구'라는 속담이 있습니다. 소셜 미디어 사이트와 메시징 애플리케이션을 포함한 기술 기업은 범죄 활동의 통로가 되거나 플랫폼에 불법적인 자료를 보유하는 것을 원하지 않습니다. 이러한 플랫폼과 서비스의 운영자는 해당 플랫폼이 운영되는 관할 지역에서 CSAM 및 기타 불법 콘텐츠의 확산을 방지하기 위해 노력합니다.
하지만 기업이 이러한 콘텐츠를 탐지하고 삭제하는 이유는 규정 준수뿐만 아니라 나머지 사용자와 사회, 비즈니스에 대한 신뢰를 보호하기 위해서이기도 합니다.

정부와 법 집행 기관은 의도하지 않은 결과를 피하기 위해 암호화에 영향을 미치는 정책과 법률에 대해

[42] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

실용적이고 신중한 접근 방식을 취해야 합니다. 정부나 법 집행 기관이 모든 유형의 백도어를 활성화하면 인터넷이 더 복잡해져 추가적인 취약점이 발생하고 모든 것이 더 안전하지 않게 됩니다.[43] 이러한 백도어에 액세스하기 위한 자격 증명이 손상되면 공격자가 법 집행 기관이 액세스할 수 있는 것과 동일한 정보에 액세스하고 암호를 해독할 수 있게 되어 치명적인 결과를 초래할 수 있습니다.

이 백서의 저자들은 이제 이 논의를 다시 생각해볼 때라고 생각합니다. 암호화 논쟁은 양측이 대립하는 양상으로 전개되어 왔지만, 실제로는 같은 적과 싸우고 있습니다. 점진적인 진전으로 초점을 전환하는 것이 필수적입니다. 이 백서의 나머지 부분에서는 담론이 바뀌지 않을 경우 발생할 수 있는 문제에 대해 다룰 것입니다.

정부 관리

기술 전문가들은 보안에 큰 영향을 주지 않으면서 암호화된 콘텐츠에 대한 액세스를 가능하게 하는 것이 거의 불가능하다는 데 동의하지만, 이러한 기술적 문제는 예외적 액세스 시스템의 거버넌스 문제와 맞물려 있습니다.[44] 수많은 법률, 많은 관할권, 수많은 이해관계자들이 테이블에 참석해야 하며, 이들은 각각 가치 있지만 종종 상반된 관점을 가지고 있습니다. 암호화된 콘텐츠에 대한 예외적 액세스를 위한 포괄적인 거버넌스 구조를 수립하려면 테이블에 누가 참석해야 하는지, 암호화된 데이터에 액세스하는 합법적인 목적, 이해관계자가 요청에 응하거나 콘텐츠를 선제적으로 공유할 수 있는 현실적인 시간 프레임 등 이견을 조율해야 합니다.

한 국가의 국경 내에서 이러한 문제 중 하나라도 해결하는 것은 어려운 일입니다. 예를 들어, 미국 내 수백, 수천 명의 법 집행기관 및 기관 직원들이 통신에 안전하게 액세스하고 암호를 해독할 수 있도록 하는 것은 엄청나게 어려운 일입니다. 아마도 FBI가 관리하는 중앙 집중식 클리어링 하우스를 만들어 조정 메커니즘 역할을 하고 연방, 주 및 지방 법 집행 기관이 이를 사용할 수 있도록 사법 메커니즘을 구축할 수 있을 것입니다. 예외적 액세스 시스템을 지원하기 위해 많은 직원을 고용하고, 암호화를 다운그레이드하거나 예외적 액세스 시스템 자체를 안전하게 유지하기 위해 노력하는 회사에서 신속한 대응을 위한 시스템을 설계할 수 있습니다. 기업이나 감독 기관은 특히 데이터 요구가 접근 금지 명령과 결합된 경우 언제, 누가, 어떤 상황에서 고객 데이터에 액세스했는지 정확하게 추적하는 데 상당한

[43] https://defense360.csis.org/bad-idea-encryption-backdoors/

[44] https://www.accessnow.org/secure-the-internet/

어려움을 겪을 수 있습니다.

각 요청을 누가 관리할 수 있는지에 대한 질문에 대한 답이 간단하지 않을 수 있기 때문에 이러한 복잡성은 국제적인 규모에서 더욱 악화될 것입니다. 이로 인해 몇몇 기업은 암호화 우회 방법이 법으로 제정되면 특정 국가에서의 비즈니스를 중단하겠다고 밝히기도 했습니다.[45]

또한 거버넌스에서는 자격 증명과 도구가 관리되는 방식도 다루어야 합니다. 공무원들이 시스템을 사용해서는 안 되는 일에 사용하지 않도록 엄격한 정책과 절차를 제정해야 합니다.[46] 많은 주요 기술 회사 및 기타 출처의 사용자 정보를 대상으로 하는 NSA의 다양한 감시 프로그램을 통해 낮은 수준의 분석가들도 아무런 감독 없이 정보에 접근할 수 있었습니다. 심지어 이 기관에는 이름까지 있었습니다: LOVEINT로, 직원들이 이러한 도구를 사용하여 연인, 배우자 및 감시 대상이 아닌 다른 사람들을 감시했습니다.[47] 최근 미국 법원은 FBI가 범죄 혐의가 있는 미국인을 포함하여 수년 동안 미국 해외 정보 데이터베이스에서 278,000회 부적절하게 정보를 검색한 사실을 발견했습니다.[48]

미국 국가안보국(NSA)의 무기화된 소프트웨어 익스플로잇을 기가바이트 규모로 유출한 개인 또는 그룹인 쉐도우 브로커스(Shadow Brokers)에서 알 수 있듯이 정부도 자체 침해에서 자유롭지 않습니다.[49] 이 침해에는 대부분의 Microsoft Windows 버전을 대상으로 하는 익스플로잇 및 해킹 도구와 전 세계 여러 은행의 SWIFT 은행 시스템에 대한 정교한 해킹의 증거가 포함되어 있습니다. 이 외에도 미국 인사관리처의 21.5%에 달하는 개인정보가 유출된 사례도 있습니다.

백만 명의 인사 기록, 미국 국립문서기록관리청의 7,600만 명의 군인 기록, 인도의 아드하르 번호 데이터 유출, 스웨덴 교통국, 미국 유권자 데이터베이스 등 다양한 사례에서 유출되었습니다.[50]

---

[45] https://www.theverge.com/23409716/signal-encryption-messaging-sms-meredith-whittaker-imessage-whatsapp-china

[46] https://www.newyorker.com/news/amy-davidson/america-through-the-n-s-a-s-prism

[47] https://slate.com/technology/2013/09/loveint-how-nsa-spies-snooped-on-girlfriends-lovers-and-first-dates.html

[48] https://www.reuters.com/world/us/fbi-misused-intelligence-database-278000-searches-court-says-2023-05-19/

[49] https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

[50] https://www.executech.com/insights/the-5-scariest-data-breaches-in-government/

암호화 백도어는 취약한 인구를 박해하는 데 사용될 수 있습니다.

거버넌스와 함께 암호화 백도어가 정치적 반대자, 종교 단체 및 기타 소수자를 탄압하기 위해 권력을 가진 사람들이 악용할 수 있다는 우려도 있습니다. 암호화는 권위주의 국가의 반체제 인사나 박해받는 인구 등 취약 계층의 언론의 자유를 보호하는 데 중요한 역할을 합니다. 역사적으로 많은 기술 기업들은 인권과 관련된 요구를 따르지 않기로 결정해 왔습니다. 예를 들어, 사용자의 성적 취향이나 정치적 활동 또는 소속에 관한 데이터를 넘기면 상당한 처벌을 받을 수 있습니다. 미국에서는 범죄와 관련이 있는 경우 법 집행 기관에 접근 권한을 부여해야 한다는 입장이지만, 다른 국가에서는 이러한 접근 권한이 인권 침해로 이어질 수 있습니다.

백도어 의무와 관련하여 기술 기업에게는 몇 가지 옵션이 있습니다. 모든 정부를 동일하게 취급하여 인권 침해에 연루될 수 있습니다. 또는 전체 정보와 인권 침해를 가능하게 할 가능성 없이 각 요청을 사례별로 평가할 수도 있습니다.[51]

역사적으로 암호화를 반대하는 주장은 범죄, 특히 취약 계층을 대상으로 한 범죄와의 전쟁에 중점을 두고 있습니다.[52] 그러나 이러한주장은 국제적으로도 정치적 반대자들을 침묵시키기 위해 사용되어 왔습니다. 올해 초 인도의 기술법에 따라 테러리스트가 사용했다는 이유로 14개의 메시징 애플리케이션이 금지되었습니다.[53] 이 금지 조치는 인도 정부로부터 청문회나 통지 없이 이루어져 플랫폼 사업자들을 놀라게 했습니다.

유엔 대표들은 억압적인 정권의 표적이 될 수 있는 개인을 보호하기 위해 암호화가 필수적이라고 주장했습니다. "암호화 도구는 인권 옹호자, 시민 사회, 언론인, 내부 고발자, 박해와 괴롭힘에 직면한 정치적 반체제 인사 등 전 세계에서 널리 사용되고 있습니다."라고 2016년 유엔 인권 고등판무관 자이드 라드 알 후세인은 말했습니다.[54] "암호화와 익명성은 표현과 의견의 자유, 프라이버시 권리를 모두 보장하는 수단으로서 필요합니다. 암호화 도구가 없으면 생명이 위험에 처할 수 있다고 말하는 것은 공상도 과장도 아닙니다. 최악의 경우 정부가 자국민의 휴대폰에 침입할 수 있는 능력은 단순히

[51] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[52] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[53] https://internetfreedom.in/14-mobile-apps-banned/

[54] http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf

기본적인 인권을 행사하는 개인을 박해하는 결과를 초래할 수 있습니다."

암호화를 통해 표적이 될 수 있는 사람들이 자유롭게 통신할 수 있습니다. "외부의 간섭으로부터 통신을 보호해야만 일반 인터넷 사용자, 인권 옹호자, 야당 정치인, 정치 활동가, 조사

언론인은 사이버 범죄는 물론 전 세계 정부의 감시로부터 자신을 보호할 수 있다"고 국제앰네스티는 2016년 보고서를 통해 밝혔습니다.[55]

기술 기업을 법 집행 기관으로 대리

최근에는 암호화 백도어를 필요로 하는 법 집행 기관과 유해한 자료가 전송되지 않도록 메시지를 스캔해야 하는 기술 회사로 논의의 중심이 옮겨가고 있습니다. 유해물을 발견하면 해당 기관에 알리는 것은 해당 기업의 몫입니다. 이는 가장 최근에 제안되어 통과된 법안의 핵심으로, 기술 기업이 사실상 법 집행 기관의 역할을 맡게 됩니다.

2021년 호주는 온라인 서비스 제공업체를 위한 기본 온라인 안전 기대치[56]를 도입하고 불법 및 제한 콘텐츠에 대한 업계 규정을 의무화하는 온라인 안전법을 통해 기존 보호를 확대 및 강화했습니다.[57] 최근에는 개빈 뉴섬 캘리포니아 주지사가 10월에 아동에 대한 "고의로 상업적 성 착취를 조장, 지원 또는 방조"하는 서비스에 대해 처벌하는 법안에 서명했습니다.[58] 유럽연합도 메시징 플랫폼이 CSAM을 검색하기를 원하지만 이러한 플랫폼의 유비쿼터스 감시를 촉진할 수 있다는 우려로 탐지 명령의 범위에서 엔드투엔드 암호화를 제외했습니다.[59]

법과 정책은 기술 기업이 CSAM 및 기타 불법 활동이 있을 수 있는 곳을 보다 적극적으로 파악하도록 장려함으로써 법 집행 기관의 정보 접근 요구와 보안 및 개인정보 보호 사이의 균형을 찾으려고 노력해 왔습니다. 그 결과, 기술 기업은 입법자와 정책 입안자들이 디지털 제품과 보관 중인 사용자 데이터를

---

[55] https://www.amnesty.nl/content/uploads/2016/03/160322_encryption_-_a_matter_of_human_rights_-_def.pdf

[56] https://www.esafety.gov.au/industry/basic-online-safety-expectations

[57] https://www.esafety.gov.au/newsroom/whats-on/online-safety-act

[58] https://www.firstpost.com/tech/news-analysis/californias-governor-signs-ban-penalising-social-media-platforms-for-aiding-or-abetting-child- abuse-13229372.html

[59] https://www.europarl.europa.eu/news/en/press-room/20231110IPR10118/child-sexual-abuse-online-effective-measures-no-mass- surveillance

보호하는 동시에 법 집행 기관과 정보 기관이 더 많은 데이터에 액세스할 수 있도록 해달라는 요구 사이에 놓이게 되었습니다.

타라 휠러와 제프리 케인은 외교협회 블로그에 “의회 의원들은 암호화 문제를 절반으로 줄이는 바람직하지 않은 임무에 착수했다”고 썼습니다.[60] “그들은 경찰이 백도어를 통해 귀하의 디지털 홈에 들어갈 수 있도록 허용하는 동시에 다른 모든 사람을 위해 암호화라는 철문을 보존할 수 있는 일련의 법적 예외를 요구하고 있습니다.” 하지만 다른 사람들이 백도어를 찾지 않을 것이라고 믿는 것은 현실적이지 않습니다.

이러한 중간 경로를 통해 기술 회사는 잠재적으로 유해한 콘텐츠를 식별하는 동시에 엔드투엔드 암호화를 유지할 수 있습니다. 그러나 전문가들은 이러한 클라이언트 측 스캐닝 기술이 "암호화의 사용자 개인 정보 보호 및 보안 보장을 허술하게 만들 것"이라고 믿습니다.[61] 종단 간 암호화 서비스에서 CSAM을 찾기 위해 작동하는 프로토타입을 구축한 사람들조차도 이러한 기술이 위험하다고 믿습니다.[62] 이러한 스캐닝 시스템은 감시 및 검열을 위해 쉽게 용도 변경될 수 있으며, 전 세계 기술 회사에 대한 요청을 통해 정치적 반체제 인사, 종교적 소수자 등을 표적으로 삼으려는 욕구가 입증되었습니다.

정부는 애초에 기술 기업을 법 집행 기관으로 대리하는 상황에 놓아서는 안 됩니다.[63] 기업에 법 집행 기관의 역할을 요구하면 중요한 경계가 모호해지고 직원들은 사용자, 기업, 정부에 대한 의무 사이에서 본질적으로 이해 상충이 발생할 수 있는 위치에 놓이게 됩니다. 또한 회사가 이러한 종류의 조사를 대리하여 수행하도록 요구받아 피해나 권리 침해에 기여한 경우 누가 책임을 져야 할지도 명확하지 않습니다.

강력한 암호화만이 범죄자를 잡을 수 있는 유일한 방법은 아닙니다.

암호화를 뚫어야 한다는 요구가 계속되고 있지만, 암호화된 디바이스와 메시지에 침입하는 것이 해커를

[60] https://www.cfr.org/blog/theres-cop-my-pocket-policymakers-need-stop-advocating-surveillance-default

[61] https://www.eff.org/deeplinks/2019/11/why-adding-client-side-scanning-breaks-end-end-encryption

[62] https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/

[63] https://www.cfr.org/blog/theres-cop-my-pocket-policymakers-need-stop-advocating-surveillance-default

잡는 최선의 방법인지는 확실하지 않습니다. 2018년 전략국제문제연구소(CSIS)는 '디지털 증거 문제에 대한 증거 기반 솔루션: 디지털 증거 문제에 대한 증거 기반 솔루션" 이 보고서는 암호화가 범죄 수사를 방해한다는 정부와 법 집행 기관의 우려는 일부 경우에 타당하지만, 단 하나의 간단한 해결책은 없다고 말합니다.[64] 실제로 연방, 주 및 지역 법 집행 기관의 설문조사 응답자들은 디지털 증거를 사건에 사용할 수 있는 능력 측면에서 가장 큰 문제로 관련 데이터를 보유한 서비스 제공업체를 식별할 수 없다는 점을 꼽았습니다(대부분 암호화되지 않음). 이 보고서는 법 집행 기관을 위한 디지털 증거 교육의 공백을 조명합니다. 여기에는 증거 수집, 증거 보관 체계 유지, 심지어 요청 절차에 중요한 역할을 하는 판사까지 포함됩니다.[65]

이러한 지식과 기술 격차는 현실 세계에 영향을 미치며, 다양한 기술의 작동 방식과 디지털 증거가 사건을 뒷받침하는 데 어떻게 사용될 수 있는지에 대한 비현실적인 기대에 잠재적으로 기여합니다. 2017년 FBI는 7,000개의 암호화된 디바이스에 침입하여 정보를 수집할 수 없다고 밝혔지만,[66] 실제로는 1,000~2,000개에 불과했습니다.[67] 그리고 FBI 수사국장의 보고서에 따르면 FBI는 샌버나디노 사건에서 법원에 애플의 해킹을 강제하기 전에 휴대폰에 접근하려고 철저히 시도하지 않았습니다.[68] 그러나 많은 경우 수사관이 바라는 것만큼 디바이스가 도움이 되지 못합니다. 영리한 범죄자들은 계획을 세우지 않고 일반인처럼 명확한 맥락 없이 짧은 메시지를 사용할 가능성이 높습니다. 종종 이러한 디바이스에는 법 집행에 도움이 될 만한 정보조차 없는 경우가 많습니다.[69]

법 집행에 대해 언급하지 않았으며, 보고서에는 대체 증거나 다른 수단을 사용하여 해결된 사건의 수가 얼마나 되는지 언급하지 않았습니다. 샌 버나디노 사건을 둘러싼 모든 논란에도 불구하고 FBI는 이 기기에서 유용한 정보를 얻지 못했습니다.[70]

---

[64] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf

[65] Ibid

[66] https://www.bbc.com/news/technology-41721354

[67] https://www.washingtonpost.com/world/national-security/fbi-repeatedly-overstated-encryption-threat-figures-to-congress- public/2018/05/22/5b68ae90-5dce-11e8-a4a4-c070ef53f315_story.html

[68] https://www.washingtonpost.com/world/national-security/inspector-general-fbi-didnt-fully-explore-whether-it-could-hack-a-terrorists-iphone- before-asking-court-to-order-apple-to-unlock-it/2018/03/27/b56a9dca-31cf-11e8-8abc-22a366b72f2d_story.html

[69] https://www.justsecurity.org/53316/criminalize-security-criminals-secure/

[70] https://www.theverge.com/2016/4/19/11463672/apple-fbi-san-bernardino-iphone-contents-no-leads

디지털 시대에 도입된 전통적인 수사 기법이 범죄자를 잡는 데 여전히 중요한 역할을 하고 있습니다. 예를 들어, 러시아 스파이 안나 채프먼은 자신의 정보를 암호화하고 비밀번호를 적어 두었는데, 이를 당국이 발견하여 정보에 액세스하는 데 사용했습니다. 불법 실크로드 시장의 우두머리를 잡기 위해 수사관들은 그가 컴퓨터에 로그인할 때까지 기다렸다가 기기를 빼앗았습니다.[71] FBI의 올라이츠법 사건에서는 해킹을 통해 휴대폰 암호를 해독하거나 심지어 친구와 가족에게 비밀번호를 공유하도록 요청하기도 했습니다.

많은 경우 특정 메시지 내용이 필요하지 않을 수 있습니다. 미국에서는 법 집행 기관과 정보 기관이 메타데이터와 트래픽 분석을 포함한 기타 데이터를 확보하여 전통적인 법적 절차를 통해 수사에 도움을 줄 수 있습니다.[72] 많은 대형 통신 서비스 제공업체가 미국에 있고 미국 법률의 적용을 받기 때문에 외국 법 집행 기관은 미국보다 훨씬 불리한 위치에 있지만, 기업은 본사가 있는 곳이 아니라 시설의 위치에 따라 요건을 적용받는 경우가 점점 더 많아지고 있기 때문에 미국은 이 점에서 유리한 위치에 있습니다. 그러나 민주 정부를 지원하는 정보 기관들 사이에도 강력한 파트너십이 존재하며, 이러한 협력은 종종 복잡한 글로벌 사건을 종결하는 데 도움이 됩니다.[73]

하지만 이러한 기술을 사용하려면 법 집행 기관이 통신 정보를 어디에서 찾을 수 있는지 알아야 합니다. 교육 센터와 디지털 증거 수집에 관한 다양한 이니셔티브에 적절한 자금을 지원하면 국가 법 집행 기관과 정보 기관뿐만 아니라 모든 수준의 법 집행 기관이 다른 문제를 야기할 수 있는 암호화 백도어에 의존하지 않고도 이러한 사건을 조사할 수 있는 역량을 갖출 수 있습니다.[74]

미국에서는 주 및 지역 법 집행관과 법률 전문가를 대상으로 디지털 증거 교육을 제공하는 국립 컴퓨터 포렌식 연구소(NCFI)에 적절한 자금을 지원하는 것이 한 단계입니다. 2018년, 행정부는 NCFI를 완전히 폐지할 것을 제안했습니다. 의회가 이를 인지하고 예산을 회복한 후에야 구출될 수 있었습니다. 그러나 이후 포렌식 교육에 대한 예산은 80% 이상 삭감되었습니다.[75] 마찬가지로 유럽연합 법 집행 협력 기구(Europol)는 유럽연합 전역의 범죄 정보 및 국가 협력을 위한 조정 허브 역할을 하며, 교육 및 디지털

[71] Ibid

[72] https://www.justsecurity.org/79549/we-now-know-what-information-the-fbi-can-obtain-from-encrypted-messaging-apps/

[73] https://www.lawfaremedia.org/article/rethinking-encryption

[74] https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf

[75] Ibid

포렌식을 위한 자원을 중앙 집중화하기에 이상적인 장소가 될 수 있습니다. 포렌식 교육은 사회의 모든 수준에서 법 집행에 도움이 될 수 있지만, 현대 수사관에게 다음과 같은 기본적이고 핵심적인 교육을 포함하는 CSAM 또는 기타 공공 위협에 대처하기 위한 제안은 거의 없습니다.

일하고 있습니다. 유사한 조직과 교육 프로그램은 범죄 활동을 수사하는 데 어려움을 겪고 있는 모든 국가의 공공 안전에 도움이 될 것입니다.[76]

법 집행 기관은 이미 확보한 디지털 증거를 관리하는 데 어려움을 겪고 있습니다. 전략 및 국제 연구 센터의 최근 보고서에 따르면 법 집행 기관 담당자를 대상으로 설문조사를 실시한 결과, 많은 사람들이 컴퓨터를 이용한 범죄뿐만 아니라 일반적인 범죄 수사에 필요한 데이터를 기술 회사에 요청하는 기본적인 방법을 실제로 알지 못하는 것으로 나타났습니다.

이러한 시스템의 데이터가 결정적인 증거가 될 것이라고 생각하기 쉽지만, 이는 잘못된 정보이거나 오탐일 가능성도 있습니다. 아일랜드 경찰청인 안 가르다 시오차나는 2010년부터 미국 국립 실종 및 착취 아동 센터(NCMEC)로부터 CSAM에 관한 정보를 받아왔습니다. 2020년에 안 가르다 시오차나는 이러한 제보 중 11% 이상이 CSAM이 아니며 해변에서 놀고 있는 어린이와 같은 무해한 이미지나 동영상 등 오탐지임을 확인했습니다.[77] 그러나 관련자들을 삭제했음에도 불구하고 안 가르다 시오차나는 이들의 데이터를 삭제하지 않았습니다. 안 가르다 시오차나의 파일이나 전 세계 다른 법 집행 기관의 파일에 CSAM 공유 혐의가 벗겨진 사람들이 얼마나 남아 있는지 알 수 없습니다.

결론

암호화는 온라인 커뮤니케이션을 보호하고, 언론의 자유를 실현하며, 금융 거래를 보호하는 등 데이터 프라이버시 및 보안에 있어 중요한 역할을 합니다. 역사적으로 암호화를 반대하는 주장은 기밀 데이터를 보호하는 동시에 공격자가 동일한 기능에 액세스하지 못하도록 막아야 한다는 것이 특징입니다. 기술은 계속 발전해 왔지만 '암호화 논쟁'은 정체되어 있습니다. 논의를 진전시키기 위해 우리는 대화를 재고하고 점진적인 발전이 혁신의 핵심이라는 사실을 받아들여야 합니다.

예외적 액세스가 CSAM 및 기타 범죄를 해결할 수 있는 유일한 방법인 것처럼 선전되어 왔지만 이는

[76] Ibid

[77] https://www.iccl.ie/news/an-garda-siochana-unlawfully-retains-files-on-innocent-people-who-it-has-already-cleared-of-producing-or-sharing- of-child-sex-abuse-material/

산만하기 짝이 없습니다. 진짜 문제는 암호화나 기술이 아니라 범죄입니다. 사이버보안 정책 및 법률 센터는 대다수의 사이버보안 커뮤니티와 함께 암호화 약화가 모든 조직과 개인의 보안, 개인정보 보호, 중요한 사회적 이익을 위태롭게 할 수 있다고 생각합니다. 이러한 범죄를 해결하는 동시에 법을 준수하는 시민의 개인정보를 보호할 수 있는 다른 솔루션과 방법도 존재합니다. 이러한 접근 방식은 전략국제문제연구소(CSIS), 카네기 국제평화재단, 프린스턴 대학교, 국제기술정책센터 등에서 주장해 왔습니다. 점진적인 진전으로 초점을 전환하는 것이 필수적입니다.