Diyaloglara Yeni bir Açıdan Bakmak: Şifreleme Tartışmasının Derinlemesine İncelenmesi

Hükûmetler, şifrelemenin yasa uygulayıcılarının işlerini yapmasına engel olduğunu söylüyor. Fakat, bu teknoloji, çocuklar ve diğer savunmasız gruplar dahil olmak üzere herkesi koruma altına alıyor.

Şubat 2024

Derleyen:
Heather West | Kıdemli Müdür
+1 202.344.4597
HEWest@Venable.com

Zack Martin | Kıdemli Politika Danışmanı
+1 202.344.4393
ZPMartin@Venable.com

Ivy Orecchio | Proje Yöneticisi
+1 202.344.4277
IDOrecchio@Venable.com

CENTER FOR CYBERSECURITY POLICY AND LAW

İçindekiler

YöneticiÖzeti

Şifreleme, diğer işlevlerinin yanında özgür ifadeyi destekleyip maddi işlemler için koruma sağlayarak çevrim içi iletişimleri korumasıyla veri gizliliği ve güvenlik bakımından kritik bir rol oynamaktadır. Siber güvenlik topluluğunun büyük çoğunluğu ile beraber Siber Güvenlik Politika ve Hukuk Merkezi, şifrelemeyi zayıflatmanın tüm kurum ve bireylerin güvenliği, gizliliği, sivil özgürlüğü ve temel sosyal çıkarlarını tehlikeye atacağına inanmaktadır.

Şifreleme, bireyleri kimlik hırsızlığı ve yasa dışı gözetim gibi suçlara karşı korusa da, emniyet teşkilatları ve ulusal güvenlik kurumları, şifrelemenin polisin suçları ve kamu güvenliğine yönelik tehditleri incelemesini daha güç ve hatta imkansız hale getirdiğini savunmaktadır. Bazıları, dijital çağda soruşturmaların, kamu güvenliği, terörizm ile ilgili ve çocukların cinsel istismarına ilişkin materyaller (CSAM) gibi yakalanan ve şifresi çözülen iletişimler dahil olmak üzere dijital kanıtları gerektirdiğini savunmaktadır.

Aslında aynı düşmanlara karşı ortak bir amaçla birleşmiş olmamıza rağmen, şifreleme karşıtları bunu iki muhalif tarafın yer aldığı bir tartışma olarak yorumlamaktadır. Şifreleme, çocuklar ve diğer savunmasız gruplar dahil olmak üzere herkesi koruma altına almaktadır. Sosyal medya siteleri ve mesajlaşma uygulamaları dahil olmak üzere teknoloji şirketleri, suç teşkil eden etkinliklere aracı olmak veya platformlarında yasa dışı malzemelere yer vermek istememektedir.

Bu araştırmanın yazarları, bu diyaloğu yeniden değerlendirmenin zamanının geldiğini düşünmektedir. Bu nedenle, hükûmet ve polisin şifrelemeyi engelleyebilen yaygın gözetim şartını koşmak yerine, kanunların yaptırımı ve çevrim içi güvenliği etkileyen politika ve mevzuatlara pratik ve kademeli bir yaklaşım benimsemesi gerekmektedir.

Bu araştırmada:

- Şifreleme politikası hakkında geçmiş tartışma ve görüşler incelenecek,
- Mevcut politikalar mevzuat bağlamında değerlendirilecek,
- Modern şifreleme tartışmasının nasıl ilerlemesi gerektiği tanımlanacak,
- Bu diyalogların değişmemesi durumunda ortaya çıkabilecek güçlükler ele alınacaktır.

Siber Güvenlik ve HukukMerkezi Hakkında

Siber Güvenlik Politika ve Kanun Merkezi, hükûmete, özel sektöreve sivil topluma güvenlikle ilgili tehditlerin daha iyi yönetilmesi için uygulama ve politikalar sağlayarak dünya çapında siber güvenliğin geliştirilmesini amaç edinen bağımsız bir kuruluştur. 2017 yılında Venable LLP'nin Siber Güvenlik Hizmetleri grubu dahilinde 501(c)(6) kategorili kâr amacı gütmeyen bir kurum olarak kurulan Merkez, koalisyonlar kurmak ve somut sonuçlar getiren girişimler başlatmak üzere küresel, ulusal ve yerel düzeylerdeki güçleri politika alanındaki uzmanlığı ile bir araya getirmektedir. Fikir birliğine yönelik ve risk yönetimi temelli bir yaklaşım uygulayan Merkez, dijital altyapı ve bilişim sistemlerinin ön cephelerinde yer alan kişilerin perspektifleri ve uygulamalarından alınan pragmatik çözümler ve politika önerilerini destekleyerek siber güvenlikle ilgili karmaşıklıklara açıklık getirmeyi ve bu konudaki kafa karışıklıklarını gidermeyi amaçlamaktadır.

Giriş

Teknoloji, günlük yaşamlarımızın ayrılmaz bir parçası haline gelmiştir. İnternet gerçekten de parmaklarımızın ucundadır. Çevirmeli telefonlar, yerini FaceTime görüşmelerine, Zoom toplantılarına bırakmış, mektuplarsa kısa mesaj ve e-postalara dönüşmüştür. Giyilebilir teknolojiler, nabzımızı, kanımızdaki şeker düzeylerini ve diğer tıbbi ölçütleri takip ederek sağlığımızla ilgili gerçek zamanlı bilgiler sağlamaktadır. İletişim teknolojileri ve Nesnelerin İnterneti, gerçekliğimizi genişletmiştir ve nerede olursak olalım arkadaşlarımız, ailelerimiz ve topluluklarımızla bağlantı kurabilmemize olanak tanımıştır. Bu dijital teknolojileri kullanım alanımız genişledikçe, şirketler sıklıkla verilerimizi korumak üzere şifrelemeden yararlanarak bu teknolojilerin güvenli kalması için sıkı çalışmalar yürütmektedir.

Dijital ortamdaki bu önemli ilerlemelerin yanında, suçlular ve kötü amaçlı kullanıcılar da bu teknolojilerden yararlanmaktadır. Polis ve ulusal güvenlik kurumları gibi toplumu korumaktan sorumlu kurumlar, yıllardır bu teknolojilerdeki güvenlik ve şifreleme mekanizmalarının işlerini yapmalarını engellediğinden endişe duymaktadır ve suçu teknoloji şirketlerine atmaktadır.

Bunu yapmak kolaydır. Sonuçta, gizlilik ve güvenlik teknolojilerimizin entegre bir parçasıdır ve giderek daha da hafife alınmaktadır. Şifreleme, önemli kişisel verilere yönelik korumaların merkezinde yer almaktadır. Polisin teklifi basittir. Bizden, şifrelenmiş materyallere erişim sağlayacak ve zararlı materyal içeren mesajları tarayacak bir sistem oluşturmamızı istemektedirler. Yetkililer, tekliflerinin çocukları korumaya, yasa dışı uyuşturucu maddeleri ortadan kaldırmaya, yolsuzluğu engellemeye yardımcı olacağını ve şiddet içeren suçları durdurma imkanı oluşturacağını söylemektedir. Ancak, bu fazlasıyla basitleştirilmiş çözümler, gizliliği tehlikeye atıp bireyleri kötü amaçlı ve görüşmeleri dinleyen kimselere maruz bırakarak oldukça tehlikeli olabilmektedir. Yine de, platformlar uçtan uca şifreleme eklemeye ve cihazlarda verileri şifrelemeye doğru ilerledikçe polis ve politika belirleyiciler, istisna aramaya devam etmektedir. Ancak, bu teklifler, şifrelemenin herkesin dijital yaşamını güvende tutmak bakımından sahip olduğu rolü yeterince önemsememektedir.

Şifreleme, bilgilerin gizli tutulması için kritik önem taşımaktadır. Şirketler, verilerini ihlallere karşı korumanın yanı sıra, iletişim ve çalışmalarını korumak üzere son elli yıldır şifrelemeden yararlanmaktadır ve birçok sektörün (sağlık, maddi hizmetler ve eğitim dahil) hukuken veya en iyi uygulamalar ve standartlar temelinde verilerini şifrelemesine yönelik endüstri gereklilikleri bulunmaktadır. Polis, ordu ve hükûmet yetkilileri de şifrelemenin önemi konusunda hemfikirdir ve kendi sistemleri ile verilerini korumak üzere aynı araç ve teknolojilerden yararlanmaktadır. Ancak, bu kamu kuruluşlarının birçoğu, çocukların ve kamu güvenliğinin korunması bahanesiyle şifrelemeyi baypas etmenin bir yolunu bulmak istemektedir. Ne yazık ki, şifreleme bir taraf için kaldırıldığında, korumak istedikleri bireyler dahil olmak üzere hemen hemen kesinlikle herkes için kaldırılmış olur.

“Şifreleme tartışmasını” veya “kripto savaşlarını” muhalif güçlerin bir çatışması olarak tanımlamak, merkezindeki ortak hedef ve karşılıklı çıkarları görmezden gelmek demektir. Bu tartışmalı konu dahilindeki kilit noktalar olan özellikle çocukların cinsel istismarı ve CSAM ile mücadele ve terör propagandası ile mücadele, teknolojik ilerlemelerden bağımsız olarak sürmektedir. Suç faaliyetleri yeni bir durum değildir ve internet ile şifrelemeden önce de var olmuştur. Sosyal medya platformları ve mesajlaşma uygulamalarını işleten teknoloji şirketleri bu tür içeriğin platformlarında olmasını istememekte ve bunu engellemek için önemli ölçüde kaynak ayırmaktadır.[1] Konu daha derinlemesine incelendiğinde, görünürde muhalif görünen bu iki taraf, ortak bir amaç altında birleşmektedir; bu amaç, çocukların ve kamunun korunması için bu suçların işlenmesini en başından önlemektir.

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

Bu ortak taahhüde karşın, ortak bir çözüm bulmaya yönelik önemli bir ilerleme henüz kaydedilememiştir. Toplumdaki bu sorunları ortadan kaldırmak için evrensel bir çözüm, kısayol veya sihirli bir değneğin olmadığını kabul etmek önemlidir. Bazı durumlarda teklif edilen çözümler, iki tarafı keskin kılıç niteliğinde olabilmektedir.

Buna örnek olarak, son zamanlarda oluşturulan bir kampanyada Apple'dan çevrim içi bulut temelli bir depolama platformu olan iCloud'da CSAM saptamaya yönelik çabalarıyla ilgili hesap sorulmaktadır. Bir reklam afişinde, "iCloud'da çocukların cinsel istismarı depolanıyor. Apple buna izin veriyor." metnine yüzü gösterilmeyen ve yapay zeka tarafından oluşturulan bir çocuk resmi eşlik etmektedir." Bu, Apple'ın iCloud'da depolanan görüntüleri taramak üzere, uçtan uca şifrelenmiş olsun olmasın CSAM saptamak üzere gizlilik ve güvenliği koruyan bir sistem geliştirme çabalarını durdurma kararına yanıt olarak ortaya çıkmıştır, ancak tam gerçekliği göstermemektedir.[2] Apple, yıllar süren araştırmaların ardından "her kullanıcının gizli olarak depolanan iCloud verilerinin taranmasının veri hırsızlarının bulup suistimal edebileceği yeni tehditler yaratacağı" kararına varmıştır. "Bu, aynı zamanda istenmeyen sonuçlara giden riskli bir durum da doğuracaktır. Örneğin, tek türden bir içeriğin taranması, kitlesel gözetimin kapısını açar ve içerik türlerinde diğer şifrelenmiş mesajlaşma sistemlerinin aranması taleplerini doğurabilir."[3]

Bu nedenle, şifreleme tartışması, karmaşıklığı ve güçlükleri ile devam etmektedir. Konununtüm tarafları bu tartışmayabasit çözümler sunarak katkı koymaktadır.. Bir yanlış anlaşılma olmasını engellemek adına tekrar vurgulamak isteriz. Siber Güvenlik Politika ve Hukuk Merkezi, çocukların ve kamunun güvenliğinin öncelikli olduğuna inanmaktadır, ancak suç ile tüm diğer kamu ve özel sektör kuruluşları ve bireylerin gizliliği ve güvenliğini tehlikeye atmadan mücadele etmenin etkili yolları bulunmaktadır. Yine de, mükemmeliyetçiliğin ilerlemenin önüne geçmesine izin veremeyiz. Potansiyel çözümleri tartışırken, gizliliği ve güvenliği artırabilecek ve topluluklarımız için koruma sağlayabilecek kademeli adımları görmezden gelmemeliyiz. Şifreleme baypasları, güvenli bir şekilde kullanılmalarını güç ve hatta imkansız hale getirebilen teknik ve politika temelli güçlüklerle doludur. Kamuyu ve çocukların güvenliğini, dijital ekosistemin tamamını ve bunu kullanan herkesi koruyan güvenliği ortadan kaldırmadan korumaya yönelik yollar olduğuna kararlılıkla inanıyoruz.

Şifrelemeyle ilgili geçmiş görüşler

Şifreciler (Sneakers) adlı, Robert Redford ve Sidney Poitier'ın başrollerinde yer aldığı 1992 yapımı filmde, bir kriptanaliz uzmanı, tüm şifreleme düzenlerini kırıp saklı her şeyin şifresini çözebilen bir cihaz geliştirmiştir. Hükûmete yönelik bilgisayar korsanlığının ardından yeni bir kimlik kullanan Robert Redford ve ekibi, yollarına bu cihazı çıkaran bir iş alır ve etik bir çıkmaza girer. Dünyanın tüm sistemlerindeki bilgilere erişme gücü parmaklarının ucundadır. Acaba bu güç çok mu fazladır? Sonunda, Redford'un ekibi bu gücün çok büyük olduğuna karar verir ve Redford cihazı imha ederek hem kötü adamlara hem de cihazın peşinde olan emniyet yetkililerine engel olur.

Bu film, 30 yılı aşkın bir süredir seyircilerin beğenisini kazanmaya devam etse de, kriptanaliz diplomasi alanında, casusluk için ve savaşların açılmasında kullanıldığından, filmin merkezinde yer alan konu yüzyıllardır tartışılmaya devam etmektedir. Tarih boyunca, gizli kodların ve şifrelerin kullanımı, güvenli iletişimin sürdürülmesi ve hassas bilgilerin korunması için gerekli olmuştur. Savaşlar kazanılıp kaybedilmiş ve suçların önüne geçilmiştir. Ancak, bunların kullanımı, potansiyel tehdit veya düşmanların aynı araç ve teknolojileri yasa dışı faaliyetler için suistimal etmesini önleme gereksinimini vurgulamaktadır.

[2] "Apple's Decision to Kill Its CSAM Photo-Scanning Tool Sparks Fresh Controversy" (Apple'ın CSAM Fotoğraf Tarama Aracını Durdurma Kararı Yeni Tartışmalar Başlattı), https://www.wired.com/story/apple-csam-scanning-heat- initiative-letter/

[3] Ibid

Modern dijital şifreleme karşıtı görüşler, kamuya açık internetin öncesinde de var olmuştur ve Soğuk Savaş sırasında önemli bir rol oynamıştır. Amerika Birleşik Devletleri, 2. Dünya Savaşı'nın ardından, iletişime yönelik şifreleme teknolojileri için, sağlam şifreleme teknolojilerinin ihraç edilmesini yasaklayan ihracat kontrolleri getirmiştir. Amerika Birleşik Devletleri'nde olduğu gibi, birçok Avrupa ülkesi de ilk zamanlar sağlam şifreleme teknolojilerine yönelik katı ihracat kontrolleri uygulamıştır ve bunları savaş malzemeleri veya askeri uygulamaları olabilen çift amaçlı ögeler olarak görmüştür.[4] Bu, belirli ölçüde başarı elde etse de genel olarak ABD dahil olmak üzere dünya çapında zayıf şifrelemenin kullanımıyla sonuçlanmıştır.

1990'larda şifreleme tartışması evrilmiştir. Ticari internetin ortaya çıkması ve kişisel bilgisayarların özellikle finansal işlemler için yaygın kullanımıyla şifreleme daha yaygın hale gelmiştir. FBI ve Ulusal Güvenlik Ajansı (NSA), uçtan uca şifreli iletişimin kullanımına karşı kamuya açık bir mücadele başlatmıştır.[6] 1993 yılında, Clipper Chip adı verilenve hükûmetin şifreli iletişimlere etişim sağlamasına izin veren bir cihaz teklif etmişlerdir.[7] Bu çip, üçüncü tarafların (bu örnekte hükûmetin) şifreli içeriği okuması için şifre çözücü bir anahtara erişim sağlamasına izin veren bir kavramdır. Sonuç olarak, zayıf ve güvenliksiz bir tasarım, sivil özgürlüklerle ilgili ve gizliliği savunan gruplardan gelen tepki karşısında başarısız olmuştur ve dolayısıyla, günümüzün telefonlarında polisin görüşmeleri dinlemesine izin veren çipler bulunmamaktadır.

1996 yılında, otuz dokuz ülke, çift amaçlı teknolojiler dahil olmak üzere ihracat kontrolleri ile ilgili Wassenaar Düzenlemesi'ni imzalamıştır. Bu anlaşma dahilinde, daha güvenliksiz şifreleme biçimleri artık ihracat kontrolüne tabi olmayacaktır.[8] Amerika Birleşik Devletleri'nde, Şifreleme ile Güvenlik ve Özgürlük (SAFE) Yasası, Soğuk Savaş dönemi politikalar nedeniyle ortaya çıkan sorunları ele almayı amaçlamıştır. Güçlü şifreleme ürünleri, yıllar boyunca sıkı düzenlemelere tabi tutulmuştur. Bunların yurt dışına satışları engellenmiştir ya da yalnızca "ihracat dereceli" daha zayıf sürümlerin satışına izin verilmiştir. İki partili bu mevzuat, ulusal güvenliği teknolojik ilerlemeler ve bireysel haklar ile dengeleme ihtiyacını vurgulamıştır. Yazılım şirketleri, mevcut ihracat kontrollerinin yeniliklerin önüne geçtiğini öne sürmüştür ve kanıtlar, yıllar önce oluşturulan politikaların etkisiz olduğunu ve ABD ekonomisinde olumsuz etki oluşturduğunu göstermiştir. [9] SAFE Yasası onaylanmasa da, 1999 yılı sonbaharında Clinton Yönetimi, yasa tasarısının neredeyse tüm hükümlerini uygulayan bir politika benimsemiştir. Bu hükümlere, perakende şifreleme ürünlerinin ihracatına yönelik sınırlandırmaların kaldırılması dahil olmuştur.[10]

NSA, bu küresel politika değişikliklerine yanıt olarak güçlü şifrelemenin altındaki şifreleme standartlarını zayıflatmak için gizli çalışmalar başlatmış ve böylece kamunun tepkisini almadan sisteme arka kapı oluşturmuştur.[11] 2006 yılına gelindiğinde, NSA, gizli sanal ağlarını kırarak halihazırda üç hava şirketinin iletişimlerine, bir seyahat rezervasyon sistemine, yabancı bir hükûmetin nükleer birimine ve başka bir hükûmetin internet hizmetine erişim sağlamıştır.

---

[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

[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/

Bu durum, 2013 Snowden sızıntılarında ortaya çıkmıştır ve casusluk ajansının şifreleme anhtarlarının oluşturulması için kullanılan rastgele sayı üreteçlerini zedeleyerek şifreli iletişimlere erişim sağladığı belgelenmiştir.[12]

Massachusetts Teknoloji Enstitüsü'nün (MIT) hazırladığı 2015 tarihli teknik bir rapor, 2000'li yıllarda bu tür şifreli içeriğe erişim sağlanmasının sorunlu olduğunu ve internetin gelişimi ve öneminin artmasıyla durumun günümüzde çok daha kötü olacağını açıkça belirtmiştir.[13] Raporda, "Milyonlarca uygulama ve küresel bakımdan bağlantılı hizmetleri içeren günümüz internet ortamının karmaşık yapısı nedeniyle, yeni kanun yaptırımı gerekliliklerinin beklenmeyen ve saptanması güç güvenlik kusurlarına yol açmasının muhtemel olduğu" belirtilmektedir. "Bunların ve diğer teknik hassasiyetlerin ötesinde, küresel düzeyde konuşlandırılmış istisnai erişim sistemleri, bu tür bir ortamın nasıl yönetilebileceği ve bu tür sistemlerin insan hakları ile hukukun üstünlüğünü nasıl gözeteceği hakkında güç sorunlar doğurmaktadır."

NSA, ağ zayıflıklarını bilgilere erişim amaçlı olarak kullanma yoluna gitmiş olsa da, FBI da bir sonraki şifreleme karşıtı mücadelede ön saflarda yer almıştır. 2015 yılında Birleşik Krallık ve ABD'deki siyasi liderler ve güvenlik teşkilatı liderleri, yeniden şifrelemeye karşı çıkmış, şifrelemenin polisin suçları incelemesine tehdit oluşturduğunu söylemiştir.[14]

Bu tartışma, San Bernardino, Kaliforniya'da yaşanan toplu silahlı saldırının ardından yeniden gündeme gelmiştir. FBI, diğer saldırganların izini sürmek üzere mahkemelerin Apple'dan silahlı saldırganın iPhone'unun PIN'ini kırmasını istemesini talep etmiştir, ancak teknoloji şirketi reddetmiştir.[15] Sonunda FBI cihazı kırabilen üçüncü taraf bir şirket bulmuştur, ancak bu durum yeniden mesajlar ve cihazlara hükûmetin arka kapılarla erişimi fikrini ön plana çıkarmıştır. Bu dönemde bir mevzuat teklif edilse de ilerleme kaydedilmemiştir. Bu, Apple'dan cihazların şifresini çözmesinin istendiği en bilinen dava olsa da tek örnek değildir. Apple'ın belirttiği ve onaylanmayan en az beş girişim daha olmuştur.[16, 17] FBI cihaza erişim sağladığında yeni herhangi bir bilgi elde etmemiştir.[18]

---

[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

[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

Tekrarlayan konular ve mevcut politika ile mevzuat

Şifreleme tartışmaları boyunca, şifreleme algoritmaları ve şifreli içeriğe yönelik arka ve ön kapılar hakkında birkaç teklif sunulmuş ve sağlam şifrelemelerin yasa dışı hale getirilmesi önerilmiştir.

Teklif	Güçlükler
Aracılı Erişim (Anahtarlı Erişim) Şifreleme anahtarlarının güvenilir üçüncü bir tarafça saklandığı, polisin belirli koşullar sağlandığında şifreli verilere erişim sağlamasına izin veren yöntemdir.	Üçüncü tarafların güvenliği ve güvenilirliği, gereksiz risklere yol açabilmektedir (örn. kötü kullanım, yetkisiz erişim). Anahtarı saklayan taraflar hedef alınırsa yıkıcı saldırılar oluşabilir. Anahtarların yeniden kurulması veya aktarılması gerektiğinde verilere hızlı erişim sağlanması güçtür.
Aracısız erişim: Polisin veri sahipleri veya işleyiciler olmadan şifreli verilere erişim sağlamak üzere araç ve tekniklerden yararlanmasıdır.	Polis tarafından kullanılan arka kapılar, aynı zamanda kötü amaçlı taraflarca veya yetkisiz kullanımlar için suistimal edilebilir. Veri konusu kişilerin bilgisi veya izni olmadan verilere erişim sağlanması, gizlilik, sivil haklar veya sivil özgürlükler bakımından çeşitli sorunlar doğurabilir.
Teknik Destek: Bir teknoloji şirketinden şifrelemeyi zayıflatarak veya verilerin şifresini çözmek üzere araçlar oluşturarak polise şifreli verilere erişim sağlamak amacıyla yardım etmesinin talep edilmesidir.	Araçların veya arka kapıların oluşturulması, sistemleri zayıflatarak saldırılara karşı daha savunmasız hale getirir. Kullanıcılar, teknoloji şirketlerinin ürünlerinin polis için özellikle zayıflatıldığına inandığında bu şirketlere olan güvenlerini kaybedebilir. Teknoloji şirketleri, uyum gerekliliklerini öngörerek başından daha zayıf sistemler oluşturabilir.

Son birkaç yıldır sunulan teklifler, polisin ve hükûmetlerin bu şifreleme saldırılarına bakış açısını değiştirmiş olsa da potansiyel etkisini değiştirmemiştir.

Birleşik Krallık'ın ÇevrimiçiÇevrimiçiGüvenlik Yasası

Eylül 2023'te Birleşik Krallık, ÇevrimiçiGüvenlik Yasası'nı onaylamıştır.[19] Bu yasa, sitelerde ve diğer internet temelli hizmetlerde yasa dışı ve zararlı malzemeler bulunmamasını sağlamayı amaçlamaktadır. Bu yasa, arama motorları, sosyal medya platformları, kullanıcının geliştirdiği içeriğe ev sahipliği yapan ortamlar, çevrim içi forumlar, oyunlar ve pornografi siteleri dahil olmak üzere geniş çaplı çevrim içi hizmet sağlayıcıları için geçerlidir.[20]

Bu Yasa, uçtan uca şifrelemeyi açık olarak yasaklamasa da, hükûmet tarafından onaylanan teknolojiler aracılığıyla içerik filtreleme ve yaş kontrolü gerektirecektir. Bu teklifte ayrıca uçtan uca mesajlaşma sağlayan teknoloji şirketlerinin mesaj içeriklerini, yetkililere bildirilmesi amacıyla CSAM kontrolü için taramasını zorunlu kılacak bir hüküm de yer almıştır.[21] Bu karar, teknoloji şirketlerinden büyük itiraz aldıysa da onaylanan yasaya getirilen ek bir değişiklik, şirketlerin "teknik bakımdan uygulanabilir hale getiriline kadar ve teknoloji yalnızca çocukların cinsel istismarı ve suistimaline yönelik içeriği saptamaya yönelik

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

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

asgari hassasiyet standartlarına ulaşıncaya kadar" şifreli mesajları taramasının gerekli olmayacağı belirtilmiştir.22 Ancak, şifreleme politikasının geçmişi, bu bakımdan polisin, teknoloji şirketlerinin ve teknoloji uzmanlarının teknik olarak neyin uygulanabilir olduğu konusunda çok farklı görüşlerinin olduğunu göstermektedir.

Popüler mesajlaşma uygulaması Signal, şifrelemeye yönelik arka kapıların gerekli görülmesi durumunda Birleşik Krallık'ta çalışmalarını durduracağını belirtmiştir.23 Birleşik Krallık İçişleri Bakanlığı da Facebook ile Instagram için uçtan uca şifreleme başlatacağını açıklayan Meta'ya karşı bir kampanya başlatmıştır ve saptanmayacağını düşündükleri CSAM'yi tanımlamak için küfürlü bir dil kullanmıştır. Bir videoda cinsel istismar kurbanı bir çocuk, Meta CEO'su Mark Zuckerberg'ten şifreleme başlatma planlarını yeniden değerlendirmesini istemiştir.24 Çevrimiçi Güvenlik Yasası'nın onaylanmasından sonra ve Birleşik Krallık İçişleri Bakanlığı'nın aksi yönde baskılarına karşın,[25] Meta, Messenger için uzun süredir planlanan uçtan uca şifrelemenin başlatacağını duyurmuş[26] ve bunun da yıl sonuna kadar şifreli WhatsApp ürünlerinin yanında yer alacağını belirtmiştir. Ayrıca, platformlarında her bir mesaja bakmalarını gerektirmeyen yöntemler kullanarak, reşit olmayanların cinsel ilişki için ikna edilmesi veya çocukların cinsel istismarına yönelik içeriğin paylaşımı konularında platformlarını kontrol etmeye devam edeceklerini söylemiştir.

Avustralya'nın Destek ve Erişim Yasası

Birleşik Krallık, mevzuat ile şifreleme kullanımını kısıtlamaya yönelik girişimlerinde yalnız değildir. Avustralya, polis ve istihbarat teşkilatlarına dijital dönemde etkin bir şekilde çalışarak terörizm ve suçları ele alması için gerekli olan araçları sağlamak üzere 2018 tarihli Destek ve Erişim Yasası'nı onaylamıştır[28]. Ancak, bu yasa çok sayıda kişi tarafından şifrelemeye bir saldırı olarak tanımlanmıştır.[29]

Bu Yasa, donanım imalatı yapan, yazılım geliştiren veya güncelleyen veya site yöneten iletişim hizmet sağlayıcılarının, işletmelerin veya bireylerin polis ve güvenlik kurumlarıyla iş birliğiiş birliği yapma sorumluluklarını artırmıştır. Ayrıca, polis için bilgisayar erişimi ruhsatları oluşturmuş ve güvenlik kurumlarının arama emri aracılığıyla hesap temelli verilere erişimi ve bilgisayar ile mobil cihazlardaki şifresiz veriler için arama ve el koyma yetkisini artırmıştır.[30]

Yasanın ana mekanizmaları arasında, verilere istisnai erişime yönelik hem gönüllülük hem de zorunluluğa dayalı talepler ile kurumlardan kendi şifrelerini kırmaları, zayıflatmaları veya arka kapılar oluşturmalarını içerebilen yeni özellikler oluşturulmasını da içeren destek talep edilmesi hükmü bulunmaktadır.[31]

---

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

[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-çevrimiçi-privacy-and-security-australia-falls-what-happens-next

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

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

Bu Yasa, onaylanma hızı, şeffaflık eksikliği ve zayıf danışmanlık süreci bakımından teknoloji şirketlerinden, gizliliği savunan kişilerden ve genel halktan eleştiri almaya devam etmektedir. Yasaya yerleştirilen önlemler hiçbir şeyin endüstriden şifrelemenin kırılmasını gerektiremeyeceğini belirtse de, eleştiren kişiler, yasanın şirketleri erişime yönelik yeni özellikler oluşturmaya zorlama yetisinin şirketleri şifrelemeyi zayıflatmaları veya arka kapılar oluşturmaları için zorlamak üzere kullanılabileceğini belirtmektedir. Avustralyalıların bilgi güvenliğinden taviz verilmesine yol açması nedeniyle bu yasanın etkisi geniş çaplı olabilir ve dünya çapında işletmelerin ve kişilerin bilgilerini tehlikeye atabilir.

Haziran 2020 itibarıyla zorunlu herhangi bir emir çıkarılmamış ve 20'nin altında destek talebi taslağı oluşturulmuştur.[32]

Diğer teklifler

Dünyanın her yerinden hükûmetler, şifreleme konusunda farklı yaklaşımlar benimsemektedir. Aşağıda, küresel olarak teklif edilen ve onaylanan politika ve mevzuatlara ilişkin özet ve potansiyel sonuçları içeren bir tablo yer almaktadır.

Ülke	Yasa	Özet	Şifreleme Üzerindeki Sonuçları
Hindistan	2000 tarihli Bilişim Teknolojisi Yasası Bölüm 69A (onaylandı)	Hindistan hükûmeti, bu yasa çerçevesinde, internet hizmet sağlayıcıları (ISP'ler) ve telekom hizmet sağlayıcıları dahil olmak üzere çevrim içi aracılara ulusal güvenliğe tehdit olarak değerlendirilen içerik veya bilgileri engelleme emrini verme yetkisine sahiptir. [33]	Bu yılın başında, Hindistan hükûmeti 14 şifreli mesajlaşma uygulamasını teröristlerin iletişimine izin verdiğini iddia ederek yasaklamak üzere kullanmış ve tüm ülkenin bu mesajlaşma uygulamalarına erişimini engellemiştir.
Avrupa Birliği	Çocukların Cinsel İstismarını Önleme ve İstismar ile Mücadele Etme amaçlı Yönetmelik (teklif edildiği adıyla Çocukların Cinsel İstismarı Yönetmeliği veya CSAR)	Bu teklif, ilk olarak sağlayıcıların hizmetlerindeki CSAM'yi saptamasını, bildirmesini ve kaldırmasını istemiştir. Bu kurallar, hizmet sağlayıcıların hizmetlerini önceden harekete geçerek CSAM ve çocukların cinsel ilişki amaçlı ikna edilmesi girişimlerine yönelik taramasını gerektirecektir.[34] Avrupa Parlamentosu'nun Sivil Özgürlük, Adalet ve İçişleri Komitesi (LIBE), bu hükmü kaldırmak ve yalnızca hedefli gözetim gerçekleştirmek üzere oylama yapmıştır.[35]	Avrupa Parlamentosu tarafından gerçekleştirilen bir etki değerlendirmesi, ilk teklifin uçtan uca şifrelemeye ve dijital iletişimin güvenliğine zarar vereceği ve geçmiş örneklere bakıldığında tüm iletişimlerin ve meta verilerin taranmasının orantısal veya gerekli görülmediğinden muhtemelen Avrupa Adalet Mahkemesi'ne ters düşeceği sonucuna varmıştır.[36] Parlamento, sonrasında saptama emirlerinin kapsamından uçtan uca şifrelemeyi çıkarmış ve bunların yalnızca diğer risk önleme tekniklerinin etkin olmaması durumunda kullanılması gerektiği netleştirmesini eklemiştir. Nihai metinde yalnızca hedefli gözetime izin verilmektedir.[37]

[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

[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] Avrupa Parlamentosu. (Nisan 2023). 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-çevrimiçi-effective-measures-no-mass- surveillance

Birleşik Krallık	Soruşturma Yetkileri Yasası (IPA) Düzenlemesine getirilen değişiklikler	IPA, olağanüstü erişime yönelik geniş çaplı gereklilikler sunmaktadır ve getirilen güncelleme, küresel piyasayı etkileyebilen yeni güvenlik güncellemelerini önceden onaylama veya engelleme yetisini içermektedir.[38]	Mevcut IPA, Birleşik Krallık hükûmetinin, şifrelemeyi zayıflatmak, sınırlandırmak veya arka kapılar açmak dahil hizmetlerini tüm kullanıcılar için değiştirmesine izin veriyor gibi görünmektedir. Ayrıca, şirketlerin hizmetlerini, uçtan uca şifreleme gibi güvenlik özelliklerinin getirilmesi dahil soruşturmaları etkileyebilecek şekilde değiştirmeden önce hükûmeti bilgilendirmesi gerekliliğini getirmektedir.
Amerika Birleşik Devletleri	Etkileşimli Teknolojilerin Kötüye Kullanım ve Kontrolsüzlük Temelli İhlallerinin Kaldırılması Yasası (EARN IT Yasası)	Bu mevzuat, Çocukların Çevrim İçi Cinsel İstismarı Ulusal Komisyonu'nu kurarak çocukların istismarını ele almayı hedeflemekte ve hizmet sağlayıcılara yönelik korumaları kaldırmak üzere İletişim Ahlak Yasası'nın 230 numaralı bölümünü değiştirerek mevcut CSAM hükümlerinin uygulanmasını pekiştirmektedir.[40]	EARN IT Yasası, hizmet sağlayıcılara, uçtan uca şifrelemeyi kaldırmaları veya arka kapılar oluşturmaları için teşvikler sunmaktadır. Bu da, çocuklar ve diğer savunmasız gruplar dahil olmak üzere tüm kullanıcılar için zayıflıklar getirmektedir. Ayrıca, teklif edilen üyelerinin çoğunluğu Kogre liderliği tarafından atandığından, Komisyon tarafından geliştirilecek en iyi uygulamalar, siyasi amaçlı olabilir.

Modern şifreleme tartışmasına açıklık getirmek

Princeton Üniversitesi Carnegie Uluslararası Barış Vakfı ve Uluslararası Teknoloji Politikası Merkezi, *yeni* yaklaşımlar bulmak amacıyla şifreleme tartışmasını derinlemesine incelemek için Şifreleme Çalışma Grubu'nu oluşturmuştur. 2019 yılında "Moving the Encryption Policy Conversation Forward" (Şifreleme Politikası Diyaloglarını İlerletmek) adlı araştırmayı yayınlamıştır.[41] Bu Grup, şifrelemenin toplum üzerindeki etkisini değerlendirmek için, polisin şifreli verilere erişimi hakkında ulaşılan çıkmaza yönelik teklif edilen tüm yaklaşımların hem faydaları hem de risklerine yer veren daha verimli yollar önermektedir. Bu araştırma, özellikle cep telefonlarındaki şifrelemeyi derinlemesine incelemekte ve polisin erişimine odaklanan tekliflerin değerlendirilmesine yönelik daha özel bir yaklaşımdan bahsetmektedir.

Bu konuya objektif ve çok paydaşlı bir bakış açısı getiren Carnegie araştırması, şifreleme lehine ve aleyhine olan iki ana görüşü reddederek giriş yapmaktadır.

1. Polis, şifreli bilgilere erişim sağlama amaçlı yaklaşımlar aramayı bırakmalıdır.
2. Polis, tüm şifreli verilere yasal bir süreç aracılığıyla erişim sağlamadan kamuyu koruyamaz.

Sonuç olarak, grup, ek çalışmaların gerçekleştirilmesi gerektiği ve ilerlemelerin cep telefonlarında şifreleme kullanımı konusunda kaydedilebileceği sonucuna varmaktadır. Buradan çıkarılabilecek noktalar arasında aşağıdakiler yer almaktadır:

- Cep telefonlarında bulunan şifreli verilerin tartışılması, farklı çıkar grupları arasında tartışmalara olanak sağlayıp risk ve faydaların daha net bir şekilde belirlenmesini sağlayacaktır.

---

[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/

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

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

- Bu alanda mevcut herhangi bir teklifin uygulanabilir olduğuna, gelecekteki tekliflerin uygulanabilir olacağına veya şu an için politika değişikliklerinin önerilebileceğine işaret bulunmamaktadır.
- Bu konu hakkında tüm taraflardan iyi niyet temelli tartışma sağlanamazsa, bu herkesi kapsayan şifreleme tartışmasında muhtemelen bir yere varılamayacaktır.

Bu bakımdan ilk önemli adım, ortak amaçların tanımlanmasıdır. Bu tartışmada hepimizin hemfikir olduğuna inandığımız bazı noktalar bulunmaktadır.

Şifreleme, çoğu kurumun verileri korumak ve kişilerin olduklarını iddia ettikleri kişiler olduğunu kanıtlamak için sahip olduğu en iyi savunmadır. Önemli veri ihlalleri yaşansa ve yaşanmaya devam edecek olsa da (Sosyal Sigorta numaralarının, ödeme kartı bilgilerinin ve diğer kişisel bilgilerin ifşa edilmesi gibi), şifreleme, bilgilerin korunması için en iyi yöntem olmaya devam etmektedir.[42] Aksi halde, suçlular bir anahtarın olduğu veya şifreleme algoritmalarının kilidini açabilecekleri bir kapısı bulunduğunu anladığında bu çok cazip bir hal alabilecektir ve bunları kendi çıkarları için kullanmak amacıyla ellerinden gelenin en iyisini yapacaklardır.

İlerlemenin püf noktası kademeli değişim olacaktır. Önceden gerçekleşen tartışmalarda aşırı basitleştirilmiş çözümler yer almıştır. Modern şifreleme tartışmaları, teknolojide gerçekleşen hızlı ilerlemelerin, bu sistemler içerisindeki karmaşıklık ve karşılıklı çalışma durumlarının ele alınmasını hareketli bir hedef haline getirdiğinin farkına varmalıdır. MIT'nin raporunda, "Yaygın ve istisnai bir erişimin elde edilmesi için dünya çapında yüz binlerce yazılımcı ile yeni teknoloji özelliklerinin kullanılıp test edilmesi gerekecektir." ifadesi yer almaktadır. "Bu, şu anda telekomünikasyon ve İnternet erişim hizmetlerinde kullanılan elektronik gözetimden çok daha karmaşık bir ortam. Telekomünikasyon ve internet erişimi hizmetlerinde genellikle benzer teknolojiler kullanılmaktadır ve bunların yeni özelliklerden kaynaklanan zayıflıkların yönetimi için kaynak bulmaları daha muhtemeldir." Şifrelemeden yararlanan ve içeriğin aktarımı veya depolanmasına yönelik ürünlerin inanılmaz sayısı, tüm istisnai erişim sorunlarının karmaşıklığını artırmış durumdadır.

Düşmanımın düşmanı dostumdur diyebiliriz. Sosyal medya siteleri ve mesajlaşma uygulamaları dahil olmak üzere teknoloji şirketleri, suç teşkil eden etkinliklere aracı olmak veya platformlarında yasa dışı içeriğe yer vermek istememektedir. Bu platform ve hizmetlerin operatörleri, çalıştıkları yetki alanlarında CSAM ve diğer yasa dışı içeriğin yayılmasını engellemek üzere çalışmalar gerçekleştirmektedir.
Ancak, bu içeriği saptamalarının ve kaldırmalarının tek nedeni kurallara uymak değildir. Kurumlar aynı zamanda kullanıcılarının geri kalanını, toplumu ve işletmelerine olan güveni de korumaktadır.

Hükûmet ve polis, istenmeyen sonuçları önlemek için şifrelemeyi etkileyen politika ve mevzuatlara pratik ve ölçülü bir yaklaşım benimsemelidir. Hükûmet veya polis için herhangi bir arka kapının açılması, interneti daha da karmaşık hale getirecek, ek zayıflıklar oluşturacak ve her şeyin daha güvensiz olmasına yol açacaktır.[43] Bu arka kapılara erişim sağlamaya yönelik giriş bilgileri ele geçirilirse sonuç felaket olacaktır ve saldırganlar polisin erişebildiği bilgilere erişip bunların şifresini çözebilecektir.

Bu araştırmanın yazarları, bu diyaloğu yeniden değerlendirmenin zamanının geldiğini düşünmektedir. Şifreleme tartışması, iki muhalif tarafın tartışması şeklinde yansıtılsa da gerçekte aynı düşmanlarla savaşmaktayız. Kademeli ilerlemeye odaklanmamız çok önemlidir. Bu araştırmanın geri kalanında, bu diyalogların değişmemesi durumunda ortaya çıkabilecek güçlükler ele alınacaktır.

---

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

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

Hükûmetin kontrol edilmesi

Teknoloji uzmanları, şifrelenmiş içeriğe güvenliği önemli ölçüde etkilemeden erişim sağlamanın neredeyse imkansız olduğu konusunda hemfikirdir. Ancak, bu bakımdan teknik güçlükler, böyle istisnai bir erişim sisteminin yönetişim güçlükleri ile el eledir.[44] Bu konuda göz önünde bulundurulması gereken sayısız yasa, birçok yetki alanı ve birçok paydaş bulunmaktadır ve bunların her biri değerli fakat birbiriyle çatışan bakış açıları sunmaktadır. Şifreli içeriğe istisnai erişimin sağlanması için kapsamlı bir yönetişim yapısının kurulması, tartışmaya kimlerin katılması gerektiği, şifreli verilere erişim sağlamak için meşru gerekçeler veya paydaşların bir talebe uyum sağlaması veya önlem amaçlı harekete geçmesine yönelik gerçekçi zaman dilimleri dahil birçok adım gerektirir.

Bu konuların tek bir tanesini tek bir ülkenin sınırları içinde çözmek bile güç bir görevdir. Örneğin, ABD içerisinde yüzlerce veya binlerce polis veya emniyet kurumu personelinin iletişimlere güvenli bir şekilde erişim sağlayıp bunların şifresini çözmesi son derece zor olacaktır. Bu amaçla, bir koordinasyonn mekanizması olarak hareket etmek üzere FBI tarafından yönetilen merkezi bir izin birimi oluşturulabilir ve bunun federal, devlet düzeyinde ve yerel polis tarafından kullanımına olanak tanımak üzere adli mekanizmalar kurulabilir. İstisnai erişim sistemlerini desteklemek, şifreleri zayıflatmak veya istisnai erişim sisteminin güvenli kalmasını sağlamak için çok çalışanlı şirketler ile hızlı yanıt temelli sistemler tasarlanabilir. Şirketler veya gözetim organları, özellikle veri talepleri medyaya açıklama yasaklarına tabi olduğunda istemci verilerine ne zaman, kimin tarafından ve hangi şartlar altında erişim sağlandığını doğru bir şekilde izlemek bakımından önemli güçlüklerle karşılaşabilir.

Her bir talebi kimin yöneteceği sorusu bu kadar basit bir şekilde yanıtlanamayacağı için bu karmaşıklık uluslararası düzeyde daha da artacaktır. Bu durum, birçok şirketin şifreleme baypasları yasal hale gelirse belirli ülkelerde işlerini durduracağını belirtmesine yol açmıştır. [45]

Ayrıca, yönetişimin erişim kimlik bilgileri ve araçlarının nasıl yönetildiğini de ele alması gerekecektir. Yetkililerin sistemi gerekenin dışında bir amaç doğrultusunda kullanmamasını sağlamak üzere katı politika ve prosedürlerin oluşturulması gerekecektir. [46] NSA'nın birçok ana teknoloji şirketi ve diğer kaynaklardan kullanıcı bilgilerini hedefleyen çeşitli gözetim programları ile düşük düzey analiz uzmanları bile herhangi bir denetim olmaksızın bilgilere erişim elde etmeyi başarmıştır. Ajans hatta buna LOVEINT adını vermiştir. Çalışanlar, LOVEINT kapsamında, gözetimi planlanmayan romantik partnerleri, eşleri ve diğer kişilerin gözetimi için bu araçlardan yararlanmıştır. [47] Daha yakın bir zamanda, ABD'deki bir mahkeme, FBI'ın, suç işlediği şüphesi bulunan Amerikalılar dahil olmak üzere birkaç yıl içerisinde 278.000 kez ABD dış işleri istihbaratı veri tabanında uygun olmayan şekilde bilgi aradığını saptamıştır. [48]

NSA'nın silah haline getirilmiş yazılım suistimaline yönelik gigabaytlarca veriyi sızdıran ve Shadow Brokers adıyla hareket eden bir kişi veya grup tarafından da kanıtlandığı gibi, hükûmetler kendi ihlallerine duyarsız değildir. [49] Bu ihlal, Microsoft Windows'un çoğu sürümünü hedef alan kötüye kullanım ve bilgisayar korsanlığı araçlarını içermiştir ve dünya çapında birkaç bankanın SWIFT bankacılık sistemine yönelik ileri düzey bilgisayar korsanlığı kanıtları bulunmaktadır. ABD Personel Yönetimi Ofisi'nin 21,5 milyon personelin

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

[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/

ABD Ulusal Arşiv ve Kayıt İdaresi'nin 76 milyon hizmet görevlisinin kaydına yönelik ihlalleri, Hindistan'ın Aadhar numaralarına yönelik veri ihlali, İsveç Ulaşım Kurumu ve ABD Seçmen Veri Tabanı ile birçok başka vakada görüldüğü gibi başka önemli örnekler de bulunmaktadır. [50]

Şifrelemelerde arka kapılar, savunmasız gruplara baskı amaçlı olarak kullanılabilir

Yönetişim ile birlikte, şifreleme arka kapılarının yetki sahibi kişiler tarafından siyasi rakiplere, dini gruplara ve diğer azınlıklara baskı uygulamak amacıyla suistimal edilebileceği kaygısıdır. Şifreleme, baskıcı yönetim şekline sahip ülkelerdeki karşıt görüşlü kişiler veya baskı gören gruplar dahil olmak üzere savunmasız grupların özgür ifade hakkının korunmasında kritik bir rol oynamaktadır. Birçok teknoloji şirketi, geçmişte de insan haklarına etki edebilecek taleplere uymamayı tercih etmiştir. Örneğin, kullanıcıların cinsel eğilimi, siyasi etkinlikleri veya tercihleri hakkında veri sağlamanın önemli cezaları olabilir. ABD'de kanun yapıcılar, bir suçla ilgili olması durumunda polise erişimin sağlanması gerektiğini önerse de başka ülkelerde böyle bir erişim insan haklarının ihlallerine yol açabilir.

Arka kapı emirleri konusunda teknoloji şirketlerinin birkaç seçeneği bulunmaktadır. Tüm hükûmetler için aynı yaklaşımı benimseyebilirler ve dolayısıyla insan haklarının ihlalinde suç ortağı haline gelebilirler. Alternatif olarak, her talebi tam bilgi vermeden ve insan haklarının ihlali olasılığına yer vermeden duruma göre değerlendirebilirler.[51]

Şifrelemeyle ilgili geçmiş iddialar, özellikle savunmasız gruplara karşı işlenen suçlar dahil suçla mücadeleye odaklanmaktadır. Ancak, bu iddialar aynı zamanda uluslararası düzeyde siyasi rakipleri susturmak için de kullanılmıştır.[52] Bu yılın başında, Hindistan'ın Teknoloji Yasası dahilinde teröristler tarafından kullanıldıkları bahanesiyle ülkede 14 mesajlaşma uygulaması yasaklanmıştır.[53] Bu yasak, herhangi bir duruşma veya Hindistan hükûmetinden herhangi bir bildirim sağlanmaksızın yürürlüğe girmiş ve platform operatörlerini saşırtmıştır.

Birleşmiş Milletler'in temsilcileri, baskıcı rejimlerce hedef alınabilecek bireylerin korunması için şifrelemenin kritik önem taşıdığı görüşünü desteklemektedir. 2016 yılında Birleşmiş Milletler İnsan Hakları Yüksek Temsilcisi Zeid Ra'ad Al Hussein, "Şifreleme araçları, insan hakları savunucuları, sivil toplum, gazeteciler, ihbarda bulunan kişiler ve zulüm ve tacizle karşı karşıya olan karşıt siyasi görüşlü kişiler dahil olmak üzere dünya çapında yaygın olarak kullanılmaktadır." diye konuşmuştur. [54] Sözlerine devam ederek, "Şifreleme ve anonimlik hem ifade ve görüş özgürlüğünün hem de gizlilik hakkının sağlanması için gereklidir." diye eklemiştir. Şifreleme araçları olmasa yaşamlar tehlikeye girebilir demek gerçek dışı veya abartılı bir ifade değildir. En kötü senaryolarda, hükûmetin vatandaşların telefonlarına izinsiz erişim sağlaması, temel insan haklarını kullanmakta olan bireylerin baskı görmesine yol açabilir."

Şifreleme, hedef alınmış olabilen kişilerin özgürce iletişim kurmasını sağlamaktadır. Uluslararası Af Örgütü'nün 2016 tarihli bir raporuna göre, "Sıradan internet kullanıcıları, insan hakları savunucuları, muhalif politikacılar, siyasi aktivistler ve araştırmacı gazeteciler kendilerini siber suçlardan ve de dünya çapında hükûmetlerin meraklı gözlerinden

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

[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

ancak müdahalesiz ve güvenli iletişim aracılığıyla koruyabilmektedir."[55]

Teknoloji şirketlerinin kanun yaptırımı için atanması

Son yıllarda, diyaloglar polisin şifreleme arka kapılarına ihtiyacı olduğu görüşünden teknoloji şirketlerinin zararlı içeriğin aktarılmadığından emin olmak üzere mesajları taraması gerekliliği görüşüne doğru değişmiştir. Bu tür içerik bulunduğunda veya bulunursa uygun yetkililere haber verme sorumluluğu teknoloji şirketlerinin olacaktır. En son teklif edilen ve onaylanan mevzuatların merkezinde bu görüş yer almaktadır ve bu da teknoloji şirketlerinin fiili olarak polisin görevini üstlenmesine neden olmaktadır.

2021 yılında, Avustralya, çevrimiçi hizmet sağlayıcıları için Temel Çevrimiçi Güvenlik Beklentilerini[56] içeren Çevrimiçi Güvenlik Yasası ile mevcut korumaları pekiştirmiş ve yasa dışı ile sınırlandırılmış içeriğe yönelik zorunlu endüstri standartları için çağrıda bulunmuştur. [57] Daha yakın zamanda ise Kaliforniya Eyaleti Başkanı Gavin Newsom, Ekim ayında, çocukların "ticari cinsel istismarına bilerek yardımcı olan ve suç ortaklığı yapan" hizmetleri cezalandıracak mevzuatı imzalamıştır. [58] Avrupa Birliği de mesajlaşma platformlarının CSAM için tarama yapmasını istemektedir, ancak bu platformlar tarafından yaygın gözetimin desteklenmesine yönelik kaygılar nedeniyle uçtan uca şifrelemeyi saptama emirlerinin kapsamından çıkarmıştır. [59]

Mevzuat ve politikalar, teknoloji şirketlerini CSAM ve diğer yasa dışı etkinlikler içerebilecek alanları saptamak konusunda daha aktif olmaya teşvik ederek polisin bilgiye erişimi gereksinimi ve güvenlik ve gizlilik arasında bir denge sağlamaya çalışmıştır. Sonuç olarak, teknoloji şirketleri, kendilerinden dijital ürünlerini güvenli hale getirmelerini isteyen kanun koyucular ve politika belirleyiciler ile sakladıkları kullanıcı verilerinin arasında kalmaktadır. Aynı zamanda, bir yandan polise ve istihbarat kurumlarına daha fazla veri için erişim sağlarken diğer yandan verileri saklamaya devam etmektedirler.

Tarah Wheeler and Geoffrey Cain, Dış İlişkiler Konseyi için bir blogda, "Kanun koyucular, şifreleme bebeğini ikiye bölmek gibi önerilmeyen bir işe girişti." ifadesini kullanmıştır. [60] "Bir yandan polisin arka kapıyı kullanarak dijital evinize girmesine izin verecek bir dizi yasal istisna talep ederken diğer herkes için şifrelemenin demir geçitlerini koruyorlar." Ancak, başkalarının arka kapı aramayacağına inanmak gerçekçi değildir.

Bu sözde orta yollar, teknoloji şirketlerinin potansiyel olarak zararlı içeriği saptarken uçtan uca şifrelemeyi korumasına olanak tanıyacaktır. Ancak, uzmanlar bu istemci taraflı tarama teknolojilerinin "kullanıcı gizliliği ve güvenliği garantilerini

---

[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-çevrimiçi-safety-expectations

[57] https://www.esafety.gov.au/newsroom/whats-on/çevrimiçi-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-çevrimiçi-effective-measures-no-mass- surveillance

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

boşa çıkaracağına" inanmaktadır.[61] Uçtan uca şifreli hizmetlerde CSAM bulmak üzere çalışan bir prototip oluşturan şirketler bile bu teknolojilerin tehlikeli olduğuna inanmaktadır.[62] Bu tür tarama sistemleri, kolaylıkla gözetim ve sansürleme amacı doğrultusunda kullanılacak şekilde değiştirilebilir ve dünya çapında teknoloji şirketlerine gelen talepler, siyasi muhalifleri, dini azınlıkları ve başkalarını hedef alma isteğini kanıtlamıştır.

Öncelikle, hükûmetlerin teknoloji şirketlerini polisin vekili haline getirmemeleri gerekmektedir.63 Şirketlerden polisin sorumluluğunu üstlenmelerini istemek, önemli bir çizgiyi belirsizleştirip teknoloji şirketlerindeki çalışanları kullanıcılara, işletmelerine ve hükûmetlere karşı görevleri arasında doğal olarak çıkar çatışmalarının bulunduğu bir konuma sürüklemektedir. Ayrıca, şirketlerin bu vekaletleri üstlenmesi ve bu tür soruşturmaları yürütmeleri istenmesi halinde haklar bakımından bir zarar veya ihlal olduğunda kimin sorumlu tutulacağı açık değildir.

Suçluluları yakalamanın tek yolu şifrelemeyi zayıflatmak değildir

Şifrelemenin kırılmasına yönelik tekrar tekrar yapılan çağrılara rağmen, şifreli cihaz ve mesajlara izinsiz erişimin, suçluların yakalanmasının en iyi yolu olduğu konusu net değildir. 2018 yılında Stratejik ve Uluslararası Araştırmalar Merkezi (CSIS), "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge" (Kolay Hedef: Dijital Kanıt Güçlüğüne Kanıt Temelli Çözümler) adlı raporu yayınlamıştır.[64] Bu raporda, hükûmet ve polisin şifrelemenin suç soruşturmalarına engel olduğu kaygısı bazı durumlarda geçerli olsa da tek ve basit bir çözümün olmadığı belirtilmektedir. Hatta, federal ile yerel düzeyde ve devlet düzeyinde emniyet görevlilerinden alınan anket yanıtları, vakalarında dijital kanıtları kullanma yetileri bakımından (çoğu şifreli olmayan) ilgili verilerin yer aldığı hizmet sağlayıcılarını belirlemenin en büyük sorun olduğunu göstermiştir. Bu rapor, polisin dijital delillere yönelik eğitimindeki açıklara ışık tutuyor. Bunlara kolektif delillerden, delil zincirinin sürdürülmesinden sorumlu personel ve hatta talep süreçleri için çok önemli olan hakimler bile dahildir.[65]

Bu bilgi ve beceri açıklığının gerçek hayatta etkileri bulunmaktadır ve çeşitli teknolojilerin nasıl işlediği ve dijital delillerin destekleyici vakalarda nasıl kullanıldığı hakkında gerçekçi olmayan beklentileri pekiştiriyor olabilirler. 2017 yılında FBI bilgi toplamak üzere 7000 şifreli cihaza erişim sağlayamadığını belirtmiştir,[66] ancak bu rakamın gerçekte bin ile iki bin arasında olduğu ortaya çıkmıştır.[67] FBI Soruşturma Müdürünün bir raporu, FBI'ın San Bernardino vakasında mahkemeden Apple'ın kırmasını istemeden önce telefona erişim sağlamayı iyice denemediğini saptamıştır.[68] Ancak, birçok vakada cihazlar soruşturmacıların umduğu kadar yararlı olmamaktadır. Deneyimli suçluların planlarını açıklaması olasılığı düşüktür ve mesajları da bizim gibi, yani pek net bir bağlam olmadan kısa ve anlık olarak kullanmaları daha muhtemeldir. Sık sık bu cihazlarda polise

---

[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

[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

yardımcı olabilecek bilgilere dahi rastlanmamaktadır [69] Raporda vakaların kaçının alternatif delillerle veya diğer yollarla çözümlendiği belirtilmemiştir. FBI, San Bernardino vakasıyla ilgili tüm tartışmaların ardından cihazdan herhangi yararlı bir bilgi elde edememiştir.[70]

Geleneksel soruşturma tekniklerinin dijital çağda suçluların yakalanmasına yönelik halen yararlı olduğu durumlar vardır. Örneğin, Rus casus Anna Chapman bilgilerini şifrelemiş ve şifrelerini bir kağıda yazmıştır. Bu kağıt daha sonra yetkililer tarafından bulunmuş ve bilgilere erişim sağlanması için kullanılmıştır. Dedektifler, yasa dışı İpek Yolu pazarının lideri olduğu iddia edilen kişiyi yakalamak için cihaza el koymadan önce bilgisayarına giriş yapmasını beklemiştir.[71] FBI'ın All Writs Act vakalarında, telefonların şifreleri, hackleme yoluyla veya arkadaşlar ya da ailelerden parolayı paylaşmalarının istenmesi yoluyla kırılmıştır.

Birçok vakada özel mesaj içerikleri gerekli olmamaktadır. ABD'de polis ve istihbarat kurumları, soruşturmalara geleneksel yasal süreçlerde yardımcı olmak üzere meta veriler ve trafik analizleri dahil başka veriler elde edebilmektedir.72 ABD'nin bu bakımdan avantajı bulunmaktadır; diğer ülkelerin emniyet teşkilatları, ABD'li muadillerine kıyasla çok daha kötü durumdadır. Bunun nedeni, en önemli iletişim hizmet sağlayıcılarının birçoğunun Amerika Birleşik Devletleri'nde bulunması ve ABD hukukuna tabi olmasıdır. Ancak, şirketler artık giderek merkezlerinin bulunduğu konumdansa tesislerinin yer aldığı konumların gerekliliklerine tabi olmaktadır. Fakat, demokrasiye dayalı hükûmetlere hizmet sağlayan istihbarat kuruluşları arasında da sağlam ortaklıklar bulunmaktadır ve küresel düzeydeki karmaşık vakalar sıklıkla iş birliği aracılığıyla çözüme kavuşturulmaktadır.[73]

Ancak, bu tekniklerin kullanılması için polisin iletişim bilgilerini nerede arayacağını bilmesi gereklidir. Eğitim merkezlerine ve çeşitli girişimlere dijital delil toplama konusunda uygun fon sağlanırsa, sadece ulusal polis teşkilatları ve istihbarat kuruluşları değil tüm düzeylerdeki emniyet teşkilatları, başka güçlüklere yol açabilecek şifreleme arka kapılarına dayanmak zorunda kalmadan bu olayları incelemek için çok daha donanımlı hale gelecektir.[74]

ABD'de, devlete ait ve yerel polise ve hukuk çalışanlarına dijital deliller hakkında eğitim sağlayan Ulusal Adli Bilişim Enstitüsü'ne (NCFI) uygun fon sağlanması buna yönelik bir adım olabilir. 2018 yılında yönetim NCFI'nın tamamen ortadan kaldırılmasını teklif etmiştir. Enstitü, ancak Kongre'nin bunu fark edip fonu yeniden etkinleştirmesiyle kurtarılmıştır. Ancak, bunu takip eden yıllarda adli bilişim eğitimlerine yönelik fonlar %80'in üzerinde kesintiye uğramıştır.[75] Benzer şekilde, Avrupa Birliği Polis Teşkilatı Kurumu Europol, AB çapında suç istihbaratı ve ulusal iş birliğine yönelik koordine bir merkez olarak çalışmaktadır ve eğitim ile dijital adli bilişim hakkındaki kaynakların merkezi hale getirilmesi için ideal bir konum olabilir. Adli bilişim eğitimleri toplumun her düzeyindeki emniyet teşkilatlarına yardımcı olabilecek olsa da, CSAM veya diğer kamusal tehditler ile mücadele için modern dedektif çalışmalarında bu temel ve kilit eğitime yer veren teklif sayısı çok azdır.

[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

[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

Benzer kuruluşlar ve eğitim programları, suç faaliyetlerinin soruşturmasında sıkıntı yaşayan her ülkede kamu güvenliğine yardımcı olacaktır.

Dijital deliller elde edildiğinde dahi polis bunların yönetimi konusunda sıkıntı yaşamaktadır. Kısa zaman önce Stratejik ve Uluslararası Çalışmalar Merkezi tarafından yayınlanan bir raporda polis memurlarına bir anket yapılmış ve birçoğunun teknoloji şirketlerine yalnızca bilgisayarlı suçlar için değil genel olarak suçlar için gerek duydukları verilere yönelik temel talepleri nasıl ileteceğini bilmediği saptanmıştır.[76]

Bu sistemlerden gelen verilerin somut deliller olacağını varsaymak kolay olsa da bunların dikkati başka yöne çekmek için kullanılması veya yalancı pozitif olma olasılığı da bulunmaktadır. İrlanda'nın ulusal polis teşkilatı An Garda Síochána, 2010 yılından beri ABD Kayıp ve İstismar Gören Çocuklar Ulusal Merkezi NCMEC'den CSAM hakkında bilgi almaktadır. 2020 yılında An Garda Síochána bu yönlendirmelerin %11'inden fazlasının CSAM olmadığını ve içeriklerin yalancı pozitif olduğunu (plajda oyun oynayan çocuklar gibi zararsız görüntü veya videolar) doğrulamıştır.[77] Ancak, An Garda Síochána ilgili kişileri temize çıkarmasına rağmen, bu kişilerin verilerini silmemiştir. CSAM paylaştığı şüphesi temize çıkarılan kaç kişinin An Garda Síochána dosyalarında veya dünya çapındaki diğer emniyet kuruluşlarının dosyalarında kaldığını bilmiyoruz.

Sonuç

Şifreleme, diğer işlevlerinin yanında özgür ifadeyi destekleyip maddi işlemler için koruma sağlayarak çevrim içi iletişimleri korumasıyla veri gizliliği ve güvenlik bakımından kritik bir rol oynamaktadır. Şifreleme karşıtı geçmiş görüşler, bir yandan kötü amaçlı grupların aynı yetkilere erişim sağlamasını engellerken diğer yandan gizli bilgilere ulaşma hedefi ile tanımlanmaktadır. Teknoloji evrilmeye devam etse de "şifreleme tartışması" hiç ilerlememiştir. Bu tartışmayı ilerletmek için bu diyalogları yeniden değerlendirmeli ve yenilikçilikte kademeli ilerlemenin kilit nokta olduğunu kabul etmemiz gereklidir.

İstisnai erişim, CSAM konusunu ve başka suçları çözüme kavuşturmanın tek yolu olarak yansıtılmış olsa da dikkatleri dağıtmaktadır; asıl sorun şifreleme veya teknoloji değil suçtur. Siber güvenlik topluluğunun büyük çoğunluğu ile beraber Siber Güvenlik Politika ve Hukuk Merkezi, şifrelemeyi zayıflatmanın tüm kurum ve bireylerin güvenliği, gizliliği ve temel sosyal çıkarlarını tehlikeye atacağına inanmaktadır. Bu suçları, yasalara uyan vatandaşların güvenliğini korumaya devam ederek çözüme kavuşturmak için başka çözüm yolları ve yöntemler bulunmaktadır. Bu yaklaşımlar, Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS) ile Princeton Üniversitesi Carnegie Uluslararası Barış Vakfı ve Uluslararası Teknoloji Politikası Merkezi tarafından savunulmaktadır. Odak noktamızı kademeli ilerlemeye yöneltmemiz çok önemlidir.

[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/