ГАНЦХАН ЧИ УНШДАГ ГЭЖ YY?

ХҮНИЙ ЭРХ БА ШИФРЛЭЛТТЭЙ ХОЛБООТОЙ АСУУДЛААР ТЕХНОЛОГИЙН 11 КОМПАНИЙГ ҮНЭЛСЭН НЬ

ЭМНЕСТИ ИНТЕРНЭШНЛ

Эмнести Интернэшнл нь 7 сая гаруй дэмжигчидтэй даян дэлхийн хөдөлгөөн бөгөөд бид хүн бүр эрхээ эдэлсэн дэлхий ертөнцийг бүтээхийн тулд кампанит ажлууд зохион байгуулдаг.

Хүний эрхийн түгээмэл тунхаглал болон бусад хүний эрхийн баримт бичгээр баталгаажсан бүх эрхийг хүн бүрт эдлүүлэхийг бид хүсдэг.

Бид аливаа Засгийн газар, улс төрийн үзэл бодол, эдийн засаг, шашны үзлээс хараат бус бөгөөд гишүүнчлэл болон олон нийтийн хандиваар санхүүждэг.

First published in October 2016
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Индекс: POL 40/4985/2016
Хэл: Англи

amnesty.org

Cover photo: Using instant messaging services is part of everyday life for hundreds of millions of people around the world, but their private communications are under real threat from cybercriminals and government surveillance. © iStock

ЭМНЕСТИ
ИНТЕРНЭШНЛ

АГУУЛГА

ТОВЧ ХУРААНГУЙ **4**

1. ОРШИЛ **7**

Хүний эрхийн асуудал болсон шифрлэлт 8

Шифрлэлт тойрсон маргаан 9

Мөшгин хяналт ба хүний эрх 10

Хувийн хэвшлийн үүрэг 10

2. ХАМРАХ ХҮРЭЭ БА АРГА ЗҮЙ **12**

3. ШАЛГУУР ҮЗҮҮЛЭЛТИЙН ЖАГСААЛТ **15**

Эрсдлийг тогтоох нь 15

Эрсдлийг бууруулах арга хэмжээ авах нь 16

Ил тод байдал 18

4. КОМПАНИУДЫН ЖАГСААЛТ **21**

5. ДҮГНЭЛТ БА ЗӨВЛӨМЖ **23**

ХАВСРАЛТ: КОМПАНИ ТУС БҮРИЙН ҮНЭЛГЭЭ **24**

Айпл (Apple) 24

Блэйкбэрри (Blackberry) 27

Фэйсбүүк (Facebook) 29

Гүүгл (Google) 33

Какао Корпораци (Kakao Corporation) 35

Лайн (LINE) 38

Майкрософт (Microsoft) 40

Снапчат (Snapchat) 42

Телеграм (Telegram) 44

Тенсэнт (Tencent) 47

Вайбер Медиа (Viber Media) 48

ТОВЧ ХУРААНГУЙ

Шифрлэлт нь цахим орчинд буй хүмүүсийн эрхийг хамгаалдаг ба хувийн мэдээллийн аюулгүй байдлыг хангадаг. Мөн цахим орчинд ямар нэг айдасгүйгээр өөрсдийн үзэл бодлоо чөлөөтэй илэрхийлэх боломжийг хүмүүст олгодог.

Шифрлэлт хүний хувийн мэдээллийг хулгайлах, цахим гэмт хэргийг таслан зогсоох, харилцаа холбоог хууль бусаар хянадаг Засгийн газрын үйл ажиллагаанаас урьдчилан сэргийлэхэд тусалдаг. Ялангуяа шифрлэлт нь Хятадын тэрс үзэлтнүүд, нутгаасаа дайжсан Бахрейны идэвхтнүүд, Европын эрэн сурвалжлах сэтгүүлчид зэрэг олон улсын хүний эрхийн хамгаалагчид, сэтгүүлчдэд их чухал хэрэгсэл юм. Мэдээлэл алдагдснаар хүмүүсийн амин чухал зүйлд сөргөөр нөлөөлж, улмаар баривчлагдах, саатуулагдахад хүргэж болно.

Тоон мэдээллийн аюулгүй байдлыг хадгалахад технологийн компаниуд чухал үүрэг хүлээдэг. Энэхүү тайланд хэрэглэгчийнхээ цахим аюулгүй байдлыг хамгаалахад ашиглаж буй технологийн 11 компаний шифрлэлт нь хүний эрхийн хүлээсэн үүрэгтэй хэр нийцэж байгаа эсэхийг харуулж, жагсаалтыг хавсаргалаа. Үүнд дэлхийн сая сая хүмүүс өдөр тутмын амьдралдаа ашигладаг Скайп (Skype), ВатсАпп (WhatsApp), ВиЧат (WeChat) зэрэг шуурхай зурвасын үйлчилгээ үзүүлэгч компаниудыг хамруулсан болно.

Шуурхай зурвасын үйлчилгээ хэрэглэж буй хүмүүсийн хувийн мэдээлэл цахим гэмт хэрэгтнүүд, хакерууд, төрийн байгууллагуудын хууль бус хяналт, аюул заналхийлэл дор байна. Бид хүний эрхийн зөрчил, эрсдлийн эсрэг ашиглаж буй шифрлэлтийн хэлбэр нь үр дүнтэй эсэхийг харуулах үүднээс тэдгээр компаний бодлого, үйл ажиллагааг анхаарч авч үзлээ. Технологийн компаниуд өөрсдийн шуурхай зурвасын үйлчилгээнд төгсгөл хоорондын шифрлэлтийг автоматаар ашиглах ёстой гэж Эмнести Интернэшнл үздэг. Учир нь энэ төрлийн шифрлэлт нь шуурхай зурвасын агуулгыг үйлчилгээ үзүүлэгч компаниуд ч тухайн мэдээлэлд нэвтрэх боломжийг хязгаарладаг.

Бидний гаргасан жагсаалтын хамгийн сүүлийн байранд Блэйкбэрри (Blackberry), Снапчат (Snapchat), Тенсэнт (Tencent) зэрэг компаниуд багтсан. Учир нь эдгээр компани өөрсдийн шуурхай зурвасын үйлчилгээнд шифрлэлтийг зохих төвшинд хэрэгжүүлдэггүй учраас хэрэглэгчдийнхээ хувийн нууцтай байх мөн үзэл бодлоо илэрхийлэх эрх чөлөөг эрсдэлд оруулдаг. Цаашлаад:

- Айпл (Apple), ЛАЙН (LINE), Вайбер Медиа (Viber Media) зэрэг гурван компани шуурхай зурвасын үйлчилгээндээ төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлдэг байна.
- Эмнести Интернэшнл бодлого, үйл ажиллагааны үзэл баримтлал нь хоорондоо зөрж байгаа таван компани байгааг олж тогтоосон юм. Тухайлбал:
- Майкрософт (Microsoft) нь хүний эрхийг хүндэтгэх тодорхой үзэл баримтлалтай хэдий ч өөрийн Скайп (Skype) үйлчилгээнд төгсгөл хоорондын шифрлэлтийн ямар ч хэлбэрийг хэрэглэдэггүй.
- Тенсэнт (Tencent) компаниас бусад нь шуурхай зурвасын үйлчилгээнд ашиглаж буй шифрлэлтэд гаргах Засгийн газрын албан шаардлагыг хүлээн зөвшөөрөхгүй хэмээн олон нийтэд мэдэгджээ.

Өнөөдөр компаниуд хувийн нууцлал, аюулгүй байдлыг дэмжихэд өөрсдийн байр суурийг олон нийтэд илэрхийлж, Засгийн газрын дарамт шахалтаас шифрлэлтийн арга хэрэгслээ

хамгаалдаг. Гэвч чансаа өндөр компаниуд хүний эрхэнд заналхийлэх явдлын эсрэг ашиглаж буй шифрлэлтийн арга хэмжээгээ өргөн хүрээнд харуулах ёстой. Энэхүү тайланд хамрагдсан бүх компани өөрсдийн ашиглаж буй шифрлэлтийг хэрэглэгчид, олон нийтэд илүү ил тод байлгах ёстой.

Одоо цагт хүний эрхийн тулгамдсан асуудлыг нааштай шийдвэрлэхэд шифрлэлт юу юунаас илүү чухал зүйл мөн. Өнөөдрийн байдлаар цахим шифрлэлтийн арга хэрэгслийг ашиглахтай холбоотой Засгийн газар, технологийн компаниуд, нууцлалыг дэмжигчид хооронд маргаан өрнөж байна. Шифрлэлт нь эрүүгийн болон терроризмын гэмт хэрэгт сэжиглэгдэж буй этгээдүүдийн тоон мэдээллийг хамгаалснаар мөрдөн шалгах ажиллагаа явуулах хууль сахиулах, батлан хамгаалах байгууллагуудын боломжийг (өөрөөр 'харанхуйн хязгаарт хүрэх' үзэгдэл гэж нэрлэдэг) маш ихээр хязгаарлаж байна гэж улс орнууд мэдэгджээ.

Улс орнууд терроризмын гэмт хэргээс ард иргэдээ хамгаалах үүрэгтэй ба олон улсын эрх зүйд нийцэж байгаа тохиолдолд гэмт хэргийг илрүүлэх зорилгоор цахим хяналт хийх эрх нь нээлттэй байдаг. Хууль ёсны зорилготой хэний ч өмнө шифрлэлт тайлагдах боломжгүй учир хууль сахиулах байгууллагын хувьд энэ нь томоохон асуудал үүсгэдэг.

Нөгөө талаар улс орнууд хувийн нууцтай байх, үзэл бодлоо илэрхийлэх эрх чөлөөг хамгаалах үүрэгтэй. Энэ нь шифрлэлтийг хязгаарлах эсвэл тойрон гарах ямар ч арга хэмжээ нь олон улсын эрх зүйд заасан хатуу шаардлагыг хангасан байх ёстой гэсэн үг юм.

Пакистан, Энэтхэг, Турк, Хятад зэрэг зарим улс орнууд шифрлэлт ашиглахыг хязгаарлах хууль тогтоомжийг хэдий нь баталгаажуулжээ. Төрийн зарим эрх бүхий байгууллагууд технологийн компаниудыг ашиглаж буй шифрлэлтэд 'арын хаалга' гаргаж, мэдээлэлд нэвтрэх тусгай боломжийг хууль сахиулах байгууллагуудад олгохыг технологийн компаниудаас шаарддаг.

Тэгвэл мэргэшсэн технологичид болон нууц үг тайлагчид төрийн эрх бүхий байгууллагуудад тусгай боломж олгох тогтолцоог бий болгох нь боломжгүй зүйл юм. Хэрэв ийм “арын хаалга” гаргах юм бол гэмт хэрэгтнүүд, хакерууд эсхүл бусад Засгийн газрууд уг боломжийг мөн адил ашиглах болно.

Шифрлэлтийн хамгаалалтад найддаг хэрэглэгчдийн цахим аюулгүй байдлыг хязгаарлах арга хэмжээнүүд нь мөн чанартаа тэнцвэргүй, олон улсын эрх зүйг зөрчсөн үйлдэл юм.

Цаашлаад, шифрлэлтийг тойрсон маргаанаас улбаалан Засгийн газрын хяналтын үйл ажиллагаанд үл итгэх хүмүүсийн тоо нэмэгдэх болно. АНУ, Их Британий тагнуулын байгууллагууд олон нийтийн сүлжээнд хяналтыг дураараа явуулж, мөн Фэйсбүүк (Facebook), Гүүгл (Google), Майкрософт (Microsoft) зэрэг компаниуд хэрэглэгчдийнхээ мэдээллийг дамжуулах нууц захиалгатай хэрхэн тулгарсан тухай 2013 онд Эдвард Сноудены илчилсэн АНУ-ын тагнуулын баримт бичигт өгүүлдэг. Яахуу (Yahoo) компани өөрийн бүх хэрэглэгчдийн цахим шууданг шалгах эрхийг АНУ-ын Засгийн газарт өгч байсан нь 2016 оны 10-р сард илчлэгджээ. Түүнчлэн ихэнх орнуудын Засгийн газар хууль ёсны үндэслэлгүйгээр идэвхтнүүд, сэтгүүлчдийн эсрэг төлөвлөгөөт хяналтын аргачлалыг ашиглаж байжээ.

Энэ тохиолдолд технологийн компаниуд өөрсдийн бүтээгдэхүүн, үйлчилгээнд мэдээллийн аюулгүй байдлын хүчирхэг хамгаалалтыг бий болгож хэрэглэгчдийнхээ эрхийн төлөө тэмцэх ёстой. Шифрлэлт ашиглахыг хязгаарлах эсхүл хориглох Засгийн газрын оролдлого нь хууль ёсны байлаа ч компаниуд эсэргүүцэх ёстой.

Энэхүү тайланд хамрагдсан компаниуд шифрлэлтийн ач холбогдлыг хэрэглэгчдийн цахим аюулгүй байдлыг хамгаалах арга хэрэгсэл гэж үздэг. Засгийн газрын арын хаалга гаргах шаардлагыг олны өмнө эсэргүүцсэн Айпл (Apple), Фэйсбүүк (Facebook) гэх мэт компаниуд өөрсдийн ашиглаж буй шифрлэлтийн аргачлалыг хүний эрхийг бодитоор эдлүүлэхэд чухал гэсэн байр сууриндаа бат зогсох ёстой. Түүнчлэн сулхан шифрлэлт ашигладаг эсхүл хүний эрхийн эрсдэлийг тооцоолдоггүй компаниуд өөрсдийн дутагдлыг засаж залруулах ёстой.

ЗУРВАСЫН НУУЦЛАЛЫН ЖАГСААЛТ

Эмнести Интернэшнл шуурхай зурвасын үйлчилгээтэй холбоотойгоор нийт хамрагдсан компаниудын ашиглаж буй шифрлэлтийн хэм хэмжээ, хүний эрхийн үүрэг хариуцлагыг тусгасан тэдний бодлого, үйл ажиллагааны талаарх дэлгэрэнгүй мэдээллийг авах зорилгоор тэдэнд ханджээ. Бидний гаргасан үнэлгээ нь тухайн компаний талаарх олон нийтэд нээлттэй мэдээлэл, мөн компани тус бүрийн хариу өгсөн байдалд үндэслэсэн.

Бид дараах таван шалгуур үзүүлэлтийн дагуу компаниудын жагсаалтыг гаргасан. Үүнд:

- Компани нь хэрэглэгчдийн хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх, эрх чөлөөг эрсдэлд оруулж буй аливаа халдлагыг эрсдэл гэж тооцон бодлого үйл ажиллагаандаа тусгасан уу?
- Компани нь төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлдэг үү?
- Компани нь хувийн нууцлал алдагдах, үзэл бодлоо илэрхийлэх эрх, эрх чөлөө нь халдлагад өртөж болох талаар хэрэглэгчиддээ ойлгуулдаг эсэх? Үүнийг шифрлэлтийн тусламжтай хэрхэн шийдвэрлэдэг вэ?
- Компани нь хэрэглэгчдийн мэдээлэл дамжуулах Засгийн газрын шаардлагыг олон нийтэд ил тод болгодог эсэх? Ямар хариу арга хэмжээ авдаг вэ?
- Компани нь өөрийн шифрлэлтийн тогтолцооны талаар техникийн дэлгэрэнгүй мэдээллийг нийтэлдэг эсэх?

Бид асуулт тус бүрт хамгийн ихдээ 3 оноо (нийт 15 оноо) өгсөн. Харин ойлгомжтой байлгах үүднээс нийт 100 хувийн босго тавьсан.

Эмнести Интернэшнл шуурхай зурвасын үйлчилгээний аюулгүй байдлыг бүхэлд нь үнэлээгүй бөгөөд харилцаа холбооны аюулгүй байдлын арга хэрэгсэл болсон ямар ч программыг баталгаажуулаагүй. Бид тоон системийн аюулгүй байдлын талаарх мэргэжлийн зөвлөгөө хүссэн сэтгүүлчид, идэвхтнүүд, хүний эрхийг хамгаалагчид эсвэл өөр хэн нэгний харилцаа холбоо эрсдэлд орж болохыг сануулсан билээ.

НИЙТ ЖАГСААЛТ

Байр	Компани	Шуурхай зурвасын үйлчилгээ	Эмнестигийн хүссэн мэдээлэлд хариу өгсөн үү?	Нийт оноо
1	Фэйсбүүк (Facebook)	ФБ Мессенжэр (FB Messenger), ВатсАпп (WhatsApp)	Тийм	73
2	Айпл(Apple)	АйМессэж (iMessage), ФэйсТайм (FaceTime)	Тийм	67
3	Телеграм (Telegram)	Телеграм Мессенжэр (Telegram Messenger)	Тийм	67
4	Гүүгл (Google)	Allo (Алло), Duo (Дуо), Хэнгаутс (Hangouts)	Үгүй	53
5	Лайн (Line)	Лайн (Line)	Тийм	47
6	Вайбер Медиа (Viber Media)	Вайбер (Viber)	Тийм	47
7	Какао (Kakao Inc)	КакаоТок (KakaoTalk)	Тийм	40
8	Майкрософт (Microsoft)	Скайп (Skype)	Тийм	40
9	Снапчат (Snapchat)	Снапчат (Snapchat)	Тийм	26
10	Блэйкбэрри (Blackberry)	Блэйкбэрри Мессенжэр (Blackberry Messenger)	Үгүй	20
11	Тенсэнт (Tencent)	КЮКЮ (QQ), ВиЧат (WeChat)	Үгүй	0

1. ОРШИЛ

Шифрлэлт нь дэлхий дахины өөрөөр сэтгэгчдийн мэдээллийг хамгаалдаг, сэтгүүлчдийг эх сурвалжтайгаа аюулгүй орчинд харилцах, дарангуйлагч дэглэмтэй улс орнуудаас төрийн бус байгууллагууд өөрсдийн ажлыг хамгаалах, өмгөөлөгчид үйлчлүүлэгчтэйгээ ганцаарчлан уулзах боломжийг олгодог чухал хэрэгсэл юм.

Цахим аюулгүй байдлын мэргэжилтэн Брюс Сшнейр, 2016 оны 2-р сар

Өнөөдрийн даяарчлагдсан ертөнцөд дэлхийн хүн амын тэн хагас нь интернэтийн технологи ашиглаж байна. Энэ нь цахим шуудан, шуурхай зурвас, олон нийтийн сүлжээгээр дамжуулан хэн нэгэнтэй харилцаа холбоо тогтоох боломж олгодог. Компаниуд мэдээллийг хадгалах, хуваалцах, аюулгүй байдлыг хангах асар их хүчин чадалтай цахим үйлчилгээг үзүүлдэг. Засгийн газрууд тоон системийн харилцаа холбооны орчинд хүний эрхийг хүндэтгэх, хамгаалах үүрэг хүлээдэг. Гэвч ихэнхдээ тэд нийтээр нь мөрдөн тандах ажиллагаа явуулах замаар өөрсдийн хүлээсэн үүргийг зөрчдөг. Үүний үр дүнд өнөөдөр дэлхийн томоохон технологийн компаниуд тоон мэдээллийн аюулгүй байдлыг хангах шифрлэлтийн асуудлаар Засгийн газар, хууль сахиулах байгууллагуудтай улс төр, технологийн маргаан хийсээр байна.

Технологийн компаниуд хүний эрхийг хүндэтгэх, хэрэглэгчдийнхээ хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөг хамгаалах үүрэгтэй. Эдгээр компаний хувьд шифрлэлт нь өөрсдийн хэрэглэгчдийн харилцаа холбооны аюулгүй байдлыг хамгаалах, хүний эрхийн эрсдлийг бууруулах хамгийн үр дүнтэй аргуудын нэг юм. Эмнести Интернэшнл цахим орчинд хүний эрхийг хамгаалахад шифрлэлтийн ач холбогдлыг тусгасан дэлгэрэнгүй нийтлэлийг өмнө нь танилцуулж байсан.[1]

Энэ тайланд хүний эрхийн асуудалд нөлөөтэй шифрлэлтэнд хандах хандлага ялангуяа өөрсдийн шуурхай зурвасын үйлчилгээнд шифрлэлтийн зохих түвшнийг хэрэгжүүлдэг эсэхэд суурилан технологийн 11 компанийг жагсаалаа. Энэхүү үйлчилгээ нь хэрэглэгчдэд текст зурвас, фото зураг, видео илгээх, аудио, видео дуудлага хийхэд интернэтийн холболт ашиглан бие биентэйгээ харилцаа холбоо тогтоох боломж олгодог.

[1] Amnesty International, Encryption: A Matter of human rights (Index POL 40/3682/2016), available at: www.amnesty.org/en/documents/pol40/3682/2016/en/

Хувь хүмүүс, хүний эрхийн идэвхтнүүд, сэтгүүлчид, олон нийт шуурхай зурвасын үйлчилгээ ашиглахад тэдний хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөө нь аюул заналхийлэлд өртдөг. Энэхүү эрсдэлтэй байдал нь олон нийтийн эсхүл төлөвлөгөөт хяналтын үйл ажиллагааны дагуу хууль бусаар олж авсан мэдээлэл, мөн олон улсын хуулийг зөрчсөн Засгийн газрын шаардлага, эсхүл үйлчилгээний аюулгүй байдалд заналхийлэх хакерууд, эрүүгийн гэмт хэрэгтнүүдээс үүдэлтэй ажээ.

ХҮНИЙ ЭРХИЙН АСУУДАЛ БОЛСОН ШИФРЛЭЛТ

Шифрлэлт нь бидний цахим мэдээлэл, харилцаа холбоог хамгаалах аргачлал юм. Энэ нь зөвхөн илгээгч, хүлээн авагч гэх хоёр тал унших боломжтойгоор мэдээллийг хөрвүүлэх математик үйлдэл бөгөөд үүнийг цахим орчинд шуудан илгээх, мөнгө санхүүгийн гүйлгээ хийх, эрүүл мэндийн мэдээллийг хадгалах зэрэг олон тохиолдолд хэрэглэдэг. Мэдээллийг шифрлэх гэдэг нь хөндлөнгийн этгээд мэдээллийг замаас нь барьж авлаа ч ойлгомжтой хэлбэрээр уншиж чадахгүй байхыг хэлнэ.

НҮБ-ын мэргэжилтэн, хүний эрхийн бүлгүүд үүний дотор Эмнести Интернэшнл шифрлэлтийг хувийн нууцтай байх эрх, үзэл бодлоо чөлөөтэй илэрхийлэх эрх, эрх чөлөөг эдлэхэд туйлын чухал ач холбогдолтой гэж үздэг.[2] Шифрлэлт нь цахим орчинд хүмүүсийг ямар нэгэн айдасгүйгээр үзэл бодол, итгэл үнэмшлээ чөлөөтэй илэрхийлэх "хувийн нууцлалын бүс" бий болгоход тусладаг.[3] Түүнчлэн тайван замаар жагсаал цуглаан, хамтын ажиллагаа зохион байгуулах эрх гэх мэт бусад эрхэд эерэг нөлөө үзүүлдэг.[4]

Энэ нь зөвхөн энгийн интернэт хэрэглэгчид, хүний эрхийг хамгаалагчид, улс төрийн сөрөг хүчин, улс төрийн идэвхтнүүд, эрэн сурвалжлах сэтгүүлчдийн харилцаа холбоог хөндлөнгийн оролцооноос хамгаалахаас гадна цахим гэмт хэрэг, Засгийн газрын мөшгин хяналтаас хамгаалдаг. НҮБ-ын Хүний эрхийн Дээд Комиссар Заед Раад Аль Хусейн хэлэхдээ "Хэлэхэд гайхмаар ч гэсэн шифрлэлтийн аргачлалгүйгээр бидний амьдрал эрсдэлд орно" хэмээжээ.[5]

Шүгэл үлээгч Эдвард Сноуден АНУ-ын Үндэсний аюулгүй байдлын агентлаг (NSA) болон Их Британий Засгийн газрын Харилцаа холбооны удирдах төв байгууллагын (GHCQ) дэлхий дахиныг хамарсан олноор нь мөрдөн тандахын хөтөлбөрүүдийг 2013 онд илчилсэн билээ.[6] Эдгээр хөтөлбөр нь дэлхий дахинд байгаа хэдэн зуун сая хүмүүсийн интернэт болон утасны дуудлагыг хянах зорилготой байжээ. Түүнчлэн, олон Засгийн газрууд идэвхтнүүд, сэтгүүлчдийг чиглэсэн хяналтыг илүүтэй гүйцэтгэдэг байжээ. Тухайлбал Этиопын Засгийн газар сөрөг хүчний идэвхтнүүдийг Этиопоос гадна ч цахимаар тагнадаг аж.[7]

Эмнести Интернэшнл үндэслэл муутай эсхүл үндэслэлгүйгээр олон нийтийг хянах эрхийг төрийн байгууллагуудад өгсөн Беларусийн нууц хяналтын системийг судалжээ. Беларусийн иргэний нийгмийн бүлгүүд ерөнхийдөө хүний эрхийг зөрчсөн хязгаарлагдмал хууль эрх зүйн орчинд үйл ажиллагаа явуулдаг.

Тус улсын идэвхтнүүдийг зүгээр л эрхээ эдлэснийх нь төлөө баривчлан, цагдан хорих арга хэмжээ авч байжээ.[8] Өөрсдийг нь хянах вий гэсэн айдас дунд амьдарч байгаа Беларусийн идэвхтнүүд болон сэтгүүлчид хэлэхдээ тэдний ажил хөдөлмөрт харилцаа холбооны шифрлэгдсэн аргачлал маш чухал ач холбогдолтой гэжээ.

[2] Amnesty International Encryption: huma rights (Index: POL 40/3682/2016), source: www.amnesty.org/en/documents/pol40/3682/2016/en/
[3] D. Kaye report 2015, p. 5.
[4] Office of the United Nations High Commissioner for Human Rights (OHCHR), Apple-FBI case could have serious global ramifications for human rights: Zeid, 4 March 2016.
[5] HR watch Ethiopia: telecom Survellance Chills Rights, 25 March 2014, wwww.hrw.org/news/2014/03/25/Ethiopia-telecom-survewilance-chills-Rights
[6] Amnesty International, "It's enough for people to feel it exists": Civil society, secrecy and surveillance in Belarus (Index: EUR 49/4306/2016).
[7] Amnesty International, What is not permitted is prohibited: Silencing civil society in Belarus (Index: EUR 49/002/2103).
[8] For example, in September 2015, the Indian government published a draft National Encryption Policy that would have required companies to store decrypted data that could be made available to law enforcement. Following extensive public criticism, the government withdrew the draft policy and is currently redrafting it. See Software Freedom Law Centre, FAQ: Legal Position of Encryption in India, 29 June 2016, available at: http://sflc.in/faq-legal-position-of-encryption-in-india/. In the USA, in April 2016, Senators Richard Burr and Dianne Feinstein released a draft encryption bill that would require companies to be able to provide decrypted data to law enforcement. See D. Feinstein, Intelligence Committee Leaders Release Discussion Draft of Encryption Bill, 13 April 2016, available at: www.feinstein.senate.gov/public/index.cfm/2016/4/intelligence-committee-leaders-release-discussion-draft-of-encryption-legislation

ШИФРЛЭЛТ ТОЙРСОН МАРГААН

Өнгөрөгч хэдхэн жил технологийн зарим компани харилцаа холбооны мэдээллийг өөрсдөө ч унших боломжгүй төгсгөл хоорондын шифрлэлтийг үйлчилгээндээ нэвтрүүлсэн юм. Энэ нь мэдээллийн аюулгүй байдлыг тойрсон олон нийтийн сэтгэл зовнидог асуудлыг шийдсэн билээ.

Үүнээс шалтгаалан хэд хэдэн улс орнууд "харанхуйн хязгаарт хүрэх" айдас хэмээх үг хэллэгтэй болжээ. Шифрлэлт нь харилцаа холбооны агуулгыг унших бидний боломжийг хязгаарлах (өөрөөр гэмт хэрэгт сэжиглэгдэж буй этгээдийг мөрдөн шалгахад шаардлагатай мэдээллийг хууль ёсны байлаа ч олж авах боломжгүй болох) болно гэж хууль сахиулах байгууллагууд үзжээ.

Тийм учраас зарим Засгийн газар болон хууль тогтоогчид арын хаалга (эрх бүхий байгууллагын шифрлэгдсэн мэдээлэл, харилцаа холбоонд нэвтрэх боломжийг дэмжих техник арга) гаргах шаардлагыг үйлчилгээ үзүүлэгчдэд тавих замаар шифрлэлтийг тойрон гарах эсхүл хязгаарлах хуулийн төслийг толилуулжээ.

Харин Пакистан, Турк, Хятад зэрэг хэд хэдэн орны Засгийн газар шифрлэлт ашиглахыг хязгаарлах хуулийг баталж амжсан.[9]

Тоон системийн аюулгүй байдлыг ноцтой зөрчих магадлалтай тохиолдол болон техник үндсэн шалтгааныг дурдан, шифрлэлтэнд арын хаалга гаргах талаарх хуулийн төслийг технологийн болон аюулгүй байдлын мэргэжилтнүүд эрс шүүмжилжээ.[10] Онцгой тохиолдолд мэдээлэл олж авах нь тоон системийн аюулгүй байдлыг хамгаалах хамгийн сайн практик туршлагынхаа эсрэг байхыг компаниудаас шаардана. Мэдээлэл олж авах механизмыг боловсруулснаар сул талыг ашиглах үүд нээж, мөн системийн бат бөх байдал алдагдаж болно. Хэрэв тодорхой байгууллага эсхүл агентлаг арын хаалга гаргах түлхүүрийг эзэмшсэн тохиолдолд тэд цахим халдлага хийх төлөвлөгөө боловсруулна. Даяарчлагдсан дэлхий ертөнцөд аливаа системийг бодит байдал дээр хэрхэн хэрэгжүүлэх тухай үндсэн зарчим байдаг.[11]

Арын хаалга гаргасан тохиолдолд гэмт хэрэгтнүүд, хакерчид эсхүл Засгийн газрууд ч мөн адил арын хаалга гаргах шаардлага тавих боломжтой болно. [12]

2016 оны 2 ба 3-р сард болсон Айпл (Apple) компани болон Холбооны Мөрдөх Товчоо (FBI) хоорондын үл ойлголцол нь шифрлэлтийг тойрсон маргааныг улам хурцатгах шалтгаан болжээ. 2015 оны 12-р сард Холбооны Мөрдөх Товчооноос (FBI) Калифорн мужийн Сан Бернардинод болсон халдлагад сэжиглэгдсэн нэг этгээдийн ашиглаж байсан Ая-фони (iPhone) утасны түгжээг тайлах хүсэлтийг тавьжээ. Засгийн газрын 'арын хаалга' гаргах шаардлага нь тодорхой нэгэн Ая-фони (iPhone) утсаас гадна бүх Ай-фоне (iPhone) утасны мэдээллийг олж авах боломжийг нээж болох учраас Айпл(Apple) компани Холбооны Мөрдөх Товчооны (FBI) шаардлагыг биелүүлэхээс татгалзжээ.

Айпл(Apple) компаний ерөнхий захирал Тим Күүк Засгийн газрын тавьсан шаардлагыг "хувийн нууцлалыг зөрчсөн" үйлдэл гэжээ.[13] Бие даасан хараат бус технологийн мэргэжилтнүүд, хууль зүйн профессорууд, технологийн компани, хүний эрхийн байгууллагууд (Эмнести Интернэшнл зэрэг) Айпл (Apple) компаний байр суурийг маш ихээр дэмждэг.[14]

Гар утас эсхүл компьютерт хадгалагдах мэдээллийг хамгаалах зорилготой төхөөрөмжийн шифрлэлтийн төрөлтэй холбоотой Айпл (Apple) болон Холбооны Мөрдөх Товчоо (FBI) хоорондын маргаант хэрэг. Хэдийгээр хууль сахиулах байгууллагууд харилцаа холбооны мэдээллийг шифрлэж буй асуудлыг шүүмжилж байгаа хэдий ч энэхүү тайлангийн үндсэн санаа нь шифрлэгдсэн зурвасыг тайлах боломжоор хангахыг компаниудаас шаардаж байгаа билээ.

---

[9] For details, see Amnesty International, *Encryption: A matter of human rights* (Index: POL 40/3682/2016), p. 12., available at: www.amnesty.org/en/documents/pol40/3682/2016/en/

[10] H. Abelson et al, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology, 6 July 2015 (hereinafter: *Keys under Doormats)*, available at: www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

[11] *Keys under Doormats*, p. 2-3.

[12] D. Kaye report 2015, para. 8.

[13] T. Cook, *A Message to Our Customers*, 16 February 2016, available at: www.apple.com/customer-letter/

[14] A list of amicus briefs in support of Apple for the 22 March 2016 hearing available at: www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

Айпл(Apple) компани Ай-Мессэж (iMessage) зурвасын үйлчилгээндээ төгсгөл хоорондын шифрлэлтийг нэвтрүүлэх шийдвэрийг Холбооны Мөрдөх Товчоо (FBI) эсэргүүцжээ.[15] Дэлхийн дахинд 1 тэрбум гаруй хэрэглэгчидтэй хамгийн том шуурхай зурвасын үйлчилгээ үзүүлэгч Фэйсбүүк (Facebook) компани 2016 оны 4-р сард ВатсАпп (WhatsApp) программдаа төгсгөл хоорондын шифрлэлтийг ашиглаж эхэлжээ.[16] ВатсАпп (WhatsApp) программд шифрлэлтийг ашиглаж эхэлсэн нь хууль сахиулах байгууллагад мэдээлэл дамжуулах асуудалтай холбоотойгоор түүнийг толгой компани болох Фэйсбүүк (Facebook)-ийн хамтаар Бразил улсын хууль эрх зүйн маргааны сэдэв болгожээ. Үүний улмаас Бразил улсын шүүгчид орон нутаг даяар ВатсАпп (WhatsApp) программыг түр хугацаанд хориглох шийдвэр гаргаж байжээ. Түүнчлэн Фэйсбүүк (Facebook) компаний удирдах ажилтанг баривчлан 24 цагийн турш цагдан хорьжээ.[17]

МӨШГИН ХЯНАЛТ БА ХҮНИЙ ЭРХ

Хувийн харилцаа холбоог хянах нь хүний эрхэд хөндлөнгөөс халдаж байгаа зүйл бөгөөд зөвхөн олон улсын эрх зүйн шалгуурыг чанд хангасан нөхцөлд хэрэгжүүлбэл зөвтгөж болохуйц зүйл. Мөн ялгаварлан гадуурхах шинж чанаргүй тэнцвэртэй байж, зөвхөн хууль ёсны зорилгод хүрэх хатуу шаардлагыг (үндэсний аюулгүй байдлыг хамгаалах, ноцтой гэмт хэрэгтэй тэмцэх гэх мэт) хангасан тохиолдолд л хэрэгжүүлэх боломжтой.

Эдвард Сноудены илчилсэн шиг тодорхой хувь хүнийг чиглээгүй, үндэслэлгүйгээр нийтээр нь тандан хянах хөтөлбөрүүд нь үргэлж хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх, эрх чөлөөнд халдсан шинж чанар агуулдаг.

Боловсронгуй шифрлэлт нь хууль ёсны зорилгоор мэдээлэл олж авах боломжийг хязгаарладаг. Засгийн газрын терроризм, цахим хяналтын гэмт хэргээс ард иргэдээ хамгаалах үүрэг нь олон улсын эрх зүйн хүрээнд нийцсэн тохиолдолд цахим хяналтыг хэрэгжүүлж болдог. Хууль бус үйл ажиллагаа явуулах зорилготой ямар ч этгээд шифрлэгдсэн мэдээллийг тайлах боломжгүй байх ёстой.[18] Үүнээс шалтгаалсан шифрлэлтийн эргэн тойрны маргаан нь хууль тогтоох байгууллагын анхаарлын төвд оршдог.

Эмнести Интернэшнл үндэслэлгүйгээр хөндлөнгөөс дур мэдэн оролцох үйл ажиллагааг хязгаарлах шифрлэлтийн аргачлалыг улс орнууд дэмжих ёстой гэж үздэг. Хууль сахиулах байгууллагын харилцаа холбооны шифрлэгдсэн мэдээлэл олж авах боломж бүрдүүлэхийн тулд шифрлэлтийг хүчгүйдүүлэх эсвэл арын хаалга гаргаж өгөхийг компаниудаас шаардах Засгийн газрын шаардлагыг олон улсын эрх зүйгээр хориглодог. Шифрлэлтийн хамгаалалтанд итгэдэг хүмүүсийн эрхийг хязгаарлахгүйгээр арын хаалга гаргах ямар ч боломжгүй.

ХУВИЙН ХЭВШЛИЙН ҮҮРЭГ

Олон улсын хүний эрхийн хэм хэмжээнд улс орнууд хүний эрхийг хамгаалж харин компаниуд хүний эрхийг хүндэтгэх үүрэгтэй гэж заасан байдаг. НҮБ-ын бизнес ба хүний эрхийн тухай удирдах зарчмын дагуу хүний эрхийг хүндэтгэх үүрэг нь "бүх аж ахуйн нэгжийн олон улсын ёс зүйн хэм хэмжээ" юм.[19]

Технологийн компаниуд нь хувь хүмүүсийн мэдээллийг олж авах, Засгийн газрын хууль бус оролдогоос сэргийлэх болон цахим гэмт хэргийн заналхийлэлтэй тулгарсан хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх, эрх чөлөөг дэмжихэд чухал үүрэгтэй.

Компаниудын хүний эрхийг хүндэтгэх үүрэг нь хүний эрхийн заналхийллийн эсрэг зохих ёсны хариу арга хэмжээ авах чадамжтай байхыг шаарддаг.

[15] The Guardian (UK), *Apple's encryption means it can't comply with US court order*, 8 September 2015.
[16] The New York Times, *Apple and other Tech companies tangle with U.S. over data access,* 7 September 2015.
[17] The New York Times, *WhatsApp is briefly shut down in Brazil for a third time*, 19 July 2016; Reuters, *Facebook exec jailed over encrypted WhatsApp data says Brazil's police treated him with respect*, 6 March 2016.
[18] B. Schneier, *iPhone encryption and the return of the crypto wars*, 6 October 2014, available at: www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html
[19] UN GPs principle 11..

Хууль бус хяналтын эрсдэл болон их хэмжээний мэдээллийн зөрчил нь олон нийтэд ил тод бөгөөд технологийн компаниуд өөрсдийн бүтээгдэхүүн, үйлчилгээнд хамгийн боловсронгуй шифрлэлт ашиглаж хэрэглэгчдийнхээ мэдээллийг хамгаалах үүрэгтэй. Шифрлэлт нь хувийн харилцаа холбооны шинж чанарыг хадгалж, цаашлаад хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөг эдлэх боломжийг олгох чухал үүрэг хүлээдэг. Технологийн компаниуд болон үйлчилгээ үзүүлэгчид өөрсдийн бүтээгдэхүүн, үйлчилгээнд сул шифрлэлт ашиглах эсхүл шифрлэлт ашиглахыг хязгаарлах Засгийн газруудын шаардлагыг биелүүлэх нь хүний эрхийн зөрчлийн шалтгаан юм.

Хэрэв хэрэглэгчдийнхээ цахим аюулгүй байдлыг хамгаалах арга хэмжээ хангалтгүй эсвэл Засгийн газруудын хууль бус хяналтын ажиллагаанд хамтарсан тохиолдолд компаний нэр хүнд бодит эрсдэлд орно. Энэ нь ерөнхийдөө АНУ-ын Призм (Prism) хөтөлбөрийн нууц захиалгын дагуу өөрсдийн хэрэглэгчдийн хувийн нууц мэдээллийг Үндэсний Аюулгүй Байдлын Агентлаг (NSA)-т дамжуулах хууль эрх зүйн шаардлагатай тулгарсан Фэйсбүүк (Facebook), Гүүгл (Google), Майкрософт (Microsoft) зэрэг компаниудыг Эдвард Сноудены илчилсний дараах үр дагавар юм. Яахүү (Yahoo) компани 2015 онд өөрийн хэрэглэгчдийн цахим шууданг шалгах эрхийг АНУ-ын Засгийн газарт өгсөн нь 2016 оны 10-р сард илчлэгдэж, одоо хүртэл сэтгэл зовниулсан асуудал хэвээр байна.[20]

[20] Reuters, *Yahoo secretly scanned customer emails for U.S. intelligence–sources*, 4 October 2016, available at: www.reuters.com/article/us-yahoo-nsa-exclusive-idUSKCN1241YT

2. ХАМРАХ ХҮРЭЭ БА АРГА ЗҮЙ

Эмнести Интернэшнл 'Шуурхай зурвасын нууцлалын жагсаалтыг' гаргахдаа хэрэглэгчдийнхээ цахим аюулгүй байдлыг хамгаалахад ашиглаж буй шифрлэлтийн аргачлал нь өөрсдийн хүлээсэн хүний эрхийн үүргийг хангаж байгаа эсэхэд үндэслэж 11 компанийг хамруулаа. Энэхүү жагсаалтад шуурхай зурвасын үйлчилгээ үзүүлэгч компаниуд багтсан болно.

Бид дараах гурван шалтгааны улмаас шуурхай зурвасын үйлчилгээг сонгосон. Нэгт, компаниуд өөрсдийн шуурхай зурвасын үйлчилгээнд хүний эрхэд халдахын эсрэг боловсронгуй шифрлэлт ашиглах нь үндэслэлтэй юм.[21]

Хоёрт, энэ төрлийн үйлчилгээг ашиглах хүмүүсийн тоо ихэссээр байна. Дэлхий дахинд ухаалаг утас ашиглах хүмүүсийн тоо хурдацтай өсөж байгаагийн зэрэгцээ ялангуяа интернэт хэрэглэгчдийн хагасаас илүү хувь нь шуурхай зурвасын үйлчилгээг өдөр тутмын хэрэглээндээ авдаг.[22] Дэлхий дахин хүний эрхийн идэвхтнүүд мэдээлэл солилцох, дэмжигчдийг идэвхжүүлэхдээ ихэвчлэн шуурхай зурвасын үйлчилгээ ашигладаг.[23]

Гуравт: шуурхай зурвасын үйлчилгээ нь шифрлэлт болон үндэсний аюулгүй байдлыг тойрсон маргааны анхаарлын төвд оршсоор ирсэн. Шифрлэлтийн аргачлалыг гар утас, бусад төхөөрмжинд ашиглах талаар АНУ-ын Холбооны Мөрдөх Товчоо (FBI)-ны дарга Жэймс Комей хэлэхдээ "энэ нь үндэсний аюулгүй байдлын хууль сахиулах ажиллагаанд асуудал үүсгэж... хамгийн наад зах нь үндэсний аюулгүй байдлыг хангах ажилд маш их нөлөөлж байна.[24] Террористууд, тэдний хамсаатнууд төгсгөл хоорондын шифрлэлттэй программуудыг ашиглах нь ихсэж байна."

Төрийн байгууллагууд хэрэглэгчдийн мэдээллээ дамжуулахыг технологийн компаниудаас шаардсаар байна. Түүнчлэн саяхан Иран улс өөрсдийн хэрэглэгчдийн бүх мэдээллийг өгөхийг шуурхай зурвасын үйлчилгээ үзүүлэгчдээс шаардсан хууль баталжээ.[25]

[21] Pew Research Center, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, 22 February 2016, available at: www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/
[22] TNS Global, *The new social frontier: Instant messaging usage jumps 12% globally*, 2015, available at: www.tnsglobal.com/pressrelease/rise-of-im
[23] Y. Atal, former UNESCO Principal Director of Social and Human Sciences, keynote address, in: *Human Rights in Changing Times*, Edited by G.P. Agarwal, S.K. Choudhary and R. Gupta, 2013, p. xix, available at: www.cambridgescholars.com/download/sample/59091
[24] Bloomberg, *FBI has sights on larger battle over encryption after Apple feud*, 11 May 2016, available at: www.bloomberg.com/news/articles/2016-05-11/fbi-has-sights-on-larger-battle-over-encryption-after-apple-feud
[25] Reuters, *Iran orders social media sites to store data inside country* , 29 May 2016, available at: www.reuters.com/article/internet-irani-dUSL8N18Q0IN

Шуурхай зурвасын үйлчилгээ үзүүлдэг олон төрлийн программууд бий. Бид энэхүү тайланд дэлхий дахинд эрчимтэй үйл ажиллагаа явуулдаг хамгийн нэр хүндтэй программуудын толгой компаниудыг сонгосон. Тухайлбал, ВатсАпп (WhatsApp) бол дэлхийн хамгийн алдартай шуурхай зурвасын үйлчилгээ үзүүлэгч программ боловч Хятадад маш бага хэрэглэгчтэй. Учир нь Хятадууд ихэвчлэн Тенсэнт (Tencent) компаний ВиЧат (WeChat) (Хятадаар Weixin гэдэг) программыг ашигладаг.[26]

Дараах хүснэгтээр судалгаанд хамрагдсан нийт 11 компани, шуурхай зурвасын үйлчилгээний программуудыг үнэлэн харуулсан.

Компани	Төв байр	Зурвасын үйлчилгээ	Идэвхтэй хэрэглэгчдийн тоо
Айпл(Apple)	АНУ	АйМессэж (iMessage), Фэйстайм (FaceTime)	Тодорхойгүй; 1 тэрбум Ай-фоне утас зарагдсан
Блэйкбэрри (Blackberry)	Канад	Блэйкберри Мессенжэр (Blackberry Messenger)	100 сая
Фэйсбүүк (Facebook)	АНУ	Фэйсбүүк Мессенжэр (Facebook Messenger), ВатсАпп (WhatsApp)	Программ тус бүр 1 тэрбум
Гүүгл (Google)	АНУ	Алло (Allo), Дуо (Duo), Хэнгаутс (Hangouts)	Программм тус бүр нь тодорхойгүй; Гүүгл нийт 2 тэрбум гаруй хэрэглэгчидтэй
Какао (Kakao Inc)	Өмнөд Солонгос	КакаоТоК (KakaoTalk)	49 сая
Лайн (Line)	Япон	Лайн (Line)	218 сая
Майкрософт (Microsoft)	АНУ	Скайп (Skype)	300 сая
Снапчат (Snapchat)	АНУ	Снапчат (Snapchat)	200 сая
Телеграм (Telegram)	Герман	Телеграм Мессенжэр (Telegram Messenger)	100 сая
Тенсэнт (Tencent)	Хятад	КЮКЮ (QQ), Вичат (WeChat)	WeChat: 697 сая; QQ: 853 сая
Вайбер Медиа (Viber Media)	Люксембург	Вайбер (Viber)	250 сая

Үнэлгээний хамрах хүрээ

Энэхүү Тайланд технологийн компаниудын шифрлэлтийн бодлого, үйл ажиллагаанд суурилах хүний эрхийн тогтолцоог ашигласан ч компаниудын хүний эрхийн болон хувийн нууцлалыг дэмжих үйл ажиллагааг бүхэлд нь үнэлэх боломжгүй юм.

Эмнести Интернэшнл үйлчилгээнд ашиглагдах криптографын шинж чанарын техникийн үнэлгээ хийгээгүй. Энэхүү тайлангийн 3-р хэсэгт дэлгэрэнгүй тайлбарласанчлан судалгаанд хамрагдсан компаниудын ашигладаг шифрлэлтийн төрлийг олж мэдэхэд хүндрэлтэй байсан. Компаниудын ашиглаж буй шифрлэлтийн төрөл нь зарчмын хувьд шифрлэлтийн бат бөх байдлыг олж мэдэх чухал зүйл юм. Гэвч бодит байдал дээр тухайн шифрлэлтийн төрлийг хэрхэн хэрэгжүүлж байгаа нь бас нэг өөр асуудал юм.

Хэдийгээр шифрлэлт нь шуурхай зурвасын үйлчилгээгээр дамжих мэдээллийг хамгаалах нэн тэргүүний сонголт ч гэлээ мэдээллийн аюулгүй байдлыг хамгаалахад дан ганц баталгаа болохгүй.

Түүнчлэн, зохих ёсны шифрлэлт нь гуравдагч талын харилцаа холбооны агуулгыг олж авах боломжийг хязгаарладаг ч МЕТАДАТА-г олж авах боломжид нөлөөлдөггүй. МЕТАДАТА гэдэг нь

[26] Tech In Asia, *WeChat blasts past 700 million monthly active users, tops China's most popular apps,* 18 April 2016, available at: www.techinasia.com/wechat-blasts-700-million-monthly-active-users-tops-chinas-popular-apps

харилцаа холбоонд хамаарах бусад төрлийн мэдээллүүд үүний дотор сүлжээнд ашиглаж байгаа төхөөрөмж, хэрэглэгчид, дуудлага хийсэн цаг хугацаа, байршил гэх мэт мэдээлэл багтана. Хэрэв бусад эх сурвалжтай холбогдсон тохиолдолд МЕТАДАТА нь харилцаа холбооны тодорхой дүр зураг гаргаж, оролцогч талуудын талаарх мэдээллийг үүсгэдэг.

Зөвхөн шифрлэлтийг анхаарч үзсэнээр шуурхай зурвасын үйлчилгээний аюулгүй байдлыг бүхэлд нь үнэлэх боломжгүй бөгөөд харилцаа холбооны аюулгүй байдлын хэрэгсэл болсон ямар ч программыг баталгаажуулаагүй болно. Эмнести Интернэшнл тоон системийн аюулгүй байдлын талаарх мэргэжлийн зөвлөгөө авахыг хүссэн сэтгүүлчид, идэвхтнүүд, хүний эрхийг хамгаалагчид, бусад хүмүүсийн харилцаа холбоо эрсдэлд орж болохыг сануулсан билээ.

Арга зүй

Эмнести Интернэшнл шуурхай зурвасын үйлчилгээтэй холбоотойгоор компаний одоогийн шифрлэлтийн хэм хэмжээ болон хүний эрхийн үүрэг, хариуцлагыг тусгасан бодлого, үйл ажиллагааны талаарх дэлгэрэнгүй мэдээлэл авах хүсэлтийг судалгаанд хамрагдсан бүх компаниудад анхлан тавихад 7 компани хариу өгсөн.

Компаниудын хариу өгсөн байдал, олон нийтэд нээлттэй мэдээллүүд, тайлангуудыг харгалзан үзсэний үр дүнд нийт үнэлгээг гаргасан болно.

Эмнести Интернэшнл судалгааны үр дүнд санал бодлоо хуваалцах боломж олгосон захидлыг бүх компани руу илгээхэд 6 компани хариу өгсөн бөгөөд уг хариу хамгийн сүүлийн үнэлгээнд ихэд нөлөөлсөн.

Эмнести Интернэшнл Блэйкбэрри (Blackberry), Гүүгл (Google), Тенсэнт (Tencent) зэрэг компаниудаас ямар ч хариу хүлээн аваагүй юм.

Эмнести Интернэшнл нууц үг тайлагч, цахим аюулгүй байдлын мэргэжилтэн Маттью Грийн, Фредерик Якобс нараас мэргэжлийн хараат бус зөвөлгөө авах хүсэлтийг тавьсан. Маттью Грийн нь Жонс Хопкинсийн Мэдээллийн Аюулгүй Байдлын Хүрээлэнгийн туслах профессор юм. Түүний судалгааны гол үндэс нь криптограф юм. Түүнчлэн тэрээр криптограф инженерчлэлийн чиглэлээр ажилладаг. Фредерик Якобс нь сигналан зурвасын программд төгсгөл хоорондын шифрлэлтийг ашиглах төслийн ахлах хөгжүүлэгчээр ажилласан туршлагатай аюулгүй байдлын инженер юм. Эдгээр мэргэжилтэн бидний арга зүй, дүгнэлт хэсэгт дурдагдсан техникийн хэд хэдэн асуудлыг тайлбарласанд Эмнести Интернэшнл талархсанаа илэрхийлэхийг хүсч байна.

Бид бүхэн таван шалгуур үзүүлэлтийн дагуу компани тус бүрийг үнэлэн олон улсын бизнесийн тодорхойлолт, хүний эрхийн хэм хэмжээг нь харгалзан үзэж, дүгнэсэн. Дараагийн бүлэгт шалгуур үзүүлэлт тус бүрийг дэлгэрэнгүй авч үзнэ.

Шалгуур үзүүлэлт тус бүр нь 0-ээс 3 хүртэлх оноотой бөгөөд хэрэв компани нь шалгуур үзүүлэлтийг бүрэн дүүрэн хангасан тохиолдолд 3 оноо, дунджаас дээгүүр бол 2 оноо, дундаж бол 1 оноо, огт үгүй бол 0 оноог тус тус авна. Компани тус бүр 5 шалгуур үзүүлэлтийн дараа хамгийн ихдээ 15 оноо авах боломжтой. Харин ойлгомжтой байлгах үүднээс 100 хувийн босго тавьсан болно.

3. ШАЛГУУР ҮЗҮҮЛЭЛТИЙН ЖАГСААЛТ

НҮБ-ын бизнес ба хүний эрхийн тухай удирдах зарчмын дагуу компаниуд өөрсдийн үйл ажиллагааны хүрээнд хүний бүхий л эрхийг хүндэтгэх үүрэг хүлээдэг.[27] Энэхүү үүрэг нь улс орны хүний эрхийн өөрийн үүргийг биелүүлэх чадамж эсвэл хүсэл эрмэлзлээс үл хамаарна. Түүнчлэн энэ нь үндэсний хууль тогтоомж, дүрэм журамд нийцсэн байна.[28] Тиймээс компаниуд хүний эрхийг хүндэтгэх тууштай бодлоготой байх хэрэгтэй. Түүнчлэн хүний эрхийн зөрчил гаргахгүй байхын тулд дахин идэвхжүүлэх алхам хийх хэрэгтэй.

Хүний эрхийн зохистой үйл ажиллагаа нь компаниудаас хүний эрхийн эрсдлийг тогтоох, урьдчилан сэргийлэх үр дүнтэй арга хэмжээ авах, түүнийгээ ил тод байлгахыг шаарддаг. НҮБ-ын бизнес ба хүний эрхийн тухай удирдах зарчмын дагуу компаниуд нь "хүний эрхийг хүндэтгэдэг "хувь хүмүүс эсвэл бүлэг хүмүүст хариуцлагын арга хэмжээ авах чадвартай гэдгээ харуулах хэрэгтэй." [29]

Технологийн компаниуд тогтоогдсон хүний эрхийн эрсдлийн эсрэг зохих хариу арга хэмжээ авах ёстой.

Шуурхай зурвасын үйлчилгээ үзүүлэгч компаниуд нь:

- Хувийн нууцтай байх, үзэл бодлоо илэрхийлэх эрх, эрх чөлөөг хүндэтгэж, хэрэглэгчдийнхээ эрхэд учрах эрсдлийг олж тогтоох ёстой.
- Шифрлэлтийн аргачлалыг ашиглах замаар хүний эрхийн эрсдлийг бууруулах арга хэмжээ авах ёстой.
- Хэрэглэгчид компаний бүтээгдэхүүн, үйлчилгээний эрсдэл, эрсдлийг бууруулахад авсан арга хэмжээ, компаний үйл ажиллагааны бодит нөлөөг үнэн зөв мэдэх боломжтой байх ёстой.

Технологийн компаниудын шифрлэгдсэн зурвасын аргачлал нь хүний эрхийн үүргийг хангаж байгаа эсэхийг үнэлэх үүднээс дараах шалгуур үзүүлэлтийг Эмнести Интернэшнл боловсруулсан юм.

ЭРСДЛИЙГ ТОГТООХ НЬ

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Компаниуд нь хүний эрхийг хүндэтгэх хүлээсэн үүрэгтээ чин үнэнч байх ёстой.[30] Энэхүү тайланд нэр дурдагдсан бүх компани хувийн нууцлалын асуудлаар тогтсон үүрэг хүлээсэн байдаг.

[27] The UNGPs were endorsed by the UN Human Rights Council in 2011. UN Office of the High Commissioner for Human Rights, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework (2011), UN Doc HR/PUB/11/04, available at: www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf
[28] UNGPs, Principle 11.
[29] UNGPs, Commentary to Principle 21.
[30] UNGPs Principle 16.

Түүнчлэн үзэл бодлоо илэрхийлэх эрх чөлөө зэрэг хүний бусад эрхүүдийг тусгаж өгөх ёстой. Хүний эрхийн зохих ёсны үйл явцын эхний шатын дагуу арга хэмжээ авахын тулд компани үйл ажиллагаа, бүтээгдэхүүн болон үйлчилгээтэй холбоотой хүний эрхийн эрсдлийг мэдэж байх ёстой. Энэ нь компаний үйл ажиллагаатай холбоотой хүний эрхэд нөлөөлөх сөрөг үр дагаврыг олж тогтооход дөхөмтэй.[31]

Цахим харилцаа холбооны хэрэглэгчдийн хувийн нууцтай байх, үзэл бодлоо илэрхийлэх эрх чөлөөнд учрах эрсдлийг олон нийт сайн мэддэг бөгөөд НҮБ-ын хэд хэдэн тайлан, тогтоол, шийдвэрт үүнийг өргөн хүрээнд анхаарч авч үздэг.[32] Олон улсын хуулиар хориотой зайлшгүй шаардлагатай, дүйцсэн байдалд (Тухайлбал, шифрлэлтэнд арын хаалга гаргахыг Засгийн газар компаниудаас шаардах) хэрэгжүүлэх тохиолдолд төрийн харилцаа холбооны хяналтаас аюул заналхийлэл ирдэг. Түүнчлэн хууран мэхлэх эсхүл сүрдүүлэх замаар хүмүүсийн мөнгийг авахын тулд мэдээлэл хайсан гэмт хэрэгтнүүд, хакерууд, хувь хүнээс мөн адил заналхийлэл ирдэг.

Технологийн компаниуд шуурхай зурвасын цахим үйлчилгээгээрээ дамжуулан хүмүүсийн хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх, эрх чөлөөний эсрэг аюул заналхийллийг илрүүлэх ёстой. Түүнчлэн тэд хувийн нууцтай байх, үзэл бодлоо илэрхийлэх эрх чөлөөг дэмжихэд зориулагдсан бодлоготой байх ёстой. Уг бодлогодоо хэрэглэгчдээ хамгаалахад ямар арга хэмжээ авах, тухайн арга хэмжээ нь аливаа заналхийллийн эсрэг хэрхэн нөлөө үзүүлэхийг тодорхой тусгасан байх ёстой.

ЭРСДЛИЙН ЭСРЭГ АРГА ХЭМЖЭЭ АВАХ НЬ

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Олон улсын бизнес ба хүний эрхийн хэм хэмжээнд заасны дагуу компаниуд үйл ажиллагаа, бүтээгдэхүүн, үйлчилгээтэй холбоотой хүний эрхийн эрсдлийг олж тогтоосны дараа тухайн заналхийллийн эсрэг "зохих ёсны арга хэмжээ" авах ёстой.[33]

Шифрлэлт нь хувийн цахим харилцаа холбооны аюулгүй байдлыг хамгаалах үр дүнтэй чухал хэрэгсэл мөн. Тийм учраас хүний эрхийн эрсдлийн эсрэг эдгээр компаниудын авах үндсэн арга хэмжээний нэг нь хүчирхэг шифрлэлтийг өөрсдийн үйлчилгээнд ашиглах явдал юм. Цахим аюулгүй байдлын мэргэжилтэн Брюс Сшнейр "Аюулгүй байдал бол шифрлэлтээс ч илүү чухал зүйл юм. Гэхдээ шифрлэлт аюулгүй байдлын чухал бүрэлдэхүүн хэсэг" гэж хэлсэн байдаг.[34]

Компаниуд тогтоогдсон эрсдлийн зохих түвшинд шифрлэлтийг ашиглах ёстой. Энэхүү шалгуур үзүүлэлт нь компаниудын өөрсдийн шуурхай зурвасын үйлчилгээнд ашиглах шифрлэлтийн төрөл нь хэрэглэгчдийн хувийн нууц болон үзэл бодлоо илэрхийлэх эрх, эрх чөлөөнд халдахын эсрэг үр дүнтэй хязгаарлах, түүнээс урьдчилан сэргийлэх боломжтой эсэхийг анхаарч үзнэ.

ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТ

Энэхүү тайланд дурдагдсан шуурхай зурвасын үйлчилгээ үзүүлэгч бүх программууд хэрэглэгч болон компаний сервэр хоорондын харилцаа холбоонд хамгийн наад зах нь тээвэрлэлтийн түвшний шифрлэлтийг ашигладаг. Уг шифрлэлтийн төрөл нь гэмт хэрэг, төрийн хяналтын үйл ажиллагааны улмаас интернэтийн орчинд дамжих мэдээлэл алдагдах эсрдлээс хамгаалдаг. Тээвэрлэлтийн түвшний шифрлэлт нь харилцаа холбооны үндсэн агуулгыг унших боломжийг үйлчилгээ үзүүлэгч компанид олгодог.

Шуурхай зурвасын үйлчилгээ үзүүлэгч компаниуд нь өөрсдийн үйлчилгээнд төгсгөл хоорондын шифрлэлтийг ашиглах ёстой гэж Эмнести Интернэшнл үздэг.

[31] UNGPs principle 18.
[32] Amnesty International, Encryption: A Matter of human rights (Index: POL 40/3682/2016), pp. 13-14, available at: www.amnesty.org/en/documents/pol40/3682/2016/en/See Amnesty International
[33] UNGPs Principle 19.
[34] B. Schneier, The importance of strong encryption to security, 25 February 2016, available at: www.schneier.com/blog/archives/2016/02/the_importance_.html

Төгсгөл хоорондын шифрлэлт нь зөвхөн мэдээлэл дамжуулагч болон хүлээн авагчид л харилцаа холбооны агуулгыг тайлах түлхүүр эзэмших боломжийг олгодог.[35]

Үүнийг ашигласнаар цахим орчинд нэвтрэх боломжтой ямар ч гуравдагч төхөөрөмж, үйлчилгээ үзүүлэгч тал зурвасын агуулгыг уншиж чадахгүй.[36]

Түүнчлэн шуурхай зурвасын үйлчилгээ үзүүлэгч программын аюулгүй байдлыг бат бөх байлгах үүрэгтэй компаний хувьд энэхүү шифрлэлт нь хэрэглэгчдийн хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөний эсрэг сөрөг үйл ажиллагаанаас урьдчилан сэргийлэх хамгийн үр дүнтэй арга зам юм. Энэ нь зөвхөн Засгийн газрын олон нийтийг хянах үйл ажиллагаанаас гадна цахим гэмт хэрэгтнүүд, мөн хакеруудаас хэрэглэгчдийн мэдээллийг хамгаалдаг.[37]

Цаашлаад технологи компаниуд хэрэглэгчийн мэдээллийн агуулгыг унших өөрсдийнхөө оролцоог хязгаарласнаар төгсгөл хоорондын шифрлэлт нь тус компаниудын хувьд хэрэглэгчдийнхээ мэдээллийг Засгийн газрын шаардлагаар дамжуулах боломжгүй гэсэн баталгаа болдог. Өөрөөр хэлбэл хакерууд, Засгийн газрын хяналтын үйл ажиллагааны өмнө үйлчилгээ үзүүлэгчдийн систем хүчин мөхөсдлөө ч мэдээллийн агуулга эрсдэлд орохгүй гэсэн үг юм.[38] Компаниуд төгсгөл хоорондын шифрлэлтийг ашигласан ч мэдээллийг хулгайлах эсхүл хянах боломжтой. Гэвч энэ нь хэрэглэгчдийн зөвхөн нэг нь гар утас эсвэл өөр бусад төхөөрөмжөөр холбоо үүсгэхэд тохиолдоно.

"Төгсгөл хоорондын шифрлэлт нь мэдээллийн аюулгүй байдлыг хангахад зориулагдсан найдвартай систем юм."

Жон Хопкинсийн их сургуулийн компьютерийн шинжлэх ухааны профессор, нууц бичээс тайлагч мэргэжилтэн Маттью Грийн

Гар утсанд зориулагдсан шуурхай зурвасын үйлчилгээ үзүүлэгч программд төгсгөл хоорондын шифрлэлт ашигладаг компаниудын хувьд энэ нь хэд хэдэн техникийн шалтгааны улмаас харьцангуй хялбар.[39] Тухайлбал хүмүүс мэдээлэл дамжуулахдаа цахим шуудан ашиглах нь ховордсон.[40] Маттью Грийн хэлэхдээ Шуурхай зурвас нь "харьцангуй хямд, өргөн ашиглагддаг технологи юм. Хэрэв та шуурхай зурвасын технологийг ашиглавал яагаад төгсгөл хоорондын шифрлэлт ашиглахгүй байгаа юм бэ гэсэн асуулт урган гарна." гэжээ.

АВТОМАТААР ХЭРЭГЖҮҮЛЭХ НЬ

Хэдий компаниуд төгсгөл хоорондын шифрлэлтийг ашиглах нь хангалттай биш ч хэрэгжүүлж байгаа шифрлэлтийн аргачлал нь аюулгүй байдалд чухал үр дүн авчирдаг. Хамгийн чухал хүчин зүйлүүдийн нэг бол хэрэв автоматаар санал болгох шифрлэлтийн хамгаалалт хүч сул байвал компаниуд төгсгөл хоорондын шифрлэлтийг үндсэн горимд хэрэгжүүлэхээр сонгох эсэх эсхүл хэрэглэгчиддээ сонголт болгон үлдээх эсэх нь ил тод ойлгомжтой байх ёстой.

Хувийн нууцлалыг дэмжигчид зурвасын үйлчилгээнд төгсгөл хоорондын шифрлэлт ашиглахаас татгалзсан компаниудыг эрс шүүмжилжээ. Гүүгл (Google) компаний шинээр гаргасан Алло болон Дуо нэртэй программуудын талаар Эдвард Сноуден хэлэхдээ "Гүүгл (Google) компани өөрийн шинэ бүтээгдэхүүн Алло программдаа төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэхээ зогсоосон нь маш аюултай байдал үүсгэсэн. Тиймээс уг программыг ашиглах хэрэггүй" гэж хэлжээ.

[35] Transport encryption and end-to-end encryption both use mathematically strong encryption, which cannot easily be broken without the decryption keys. But with end-to-end, the service provider doesn't hold the key – meaning it is more effective to protect against threats to privacy on instant messaging apps.
[36] See for example, The Financial Times, 'State-sponsored actor' stole data from 500m Yahoo users, 23 September 2016; Washington Post,Chinese hackers who breached Google gained access to sensitive data, U.S. officials say, 20 May 2013; Keys under Doormats pp. 9-10.
[37] Email correspondence with cryptographers and cybersecurity specialists Matthew Green, Assistant Professor at Johns Hopkins Information Security Institute, and security engineer Frederic Jacobs, August 2016
[38] Email correspondence with Frederic Jacobs and Matthew Green, August 2016.
[39] Email correspondence with Matthew Green, August 2016.
[40] ZDNet, NSA whistleblower Snowden: Google Allo without default encryption is 'dangerous', 20 May 2016.

Төгсгөл хоорондын шифрлэлтийг автоматаар ашиглах боломжгүй байна гэдэг нь хэрэглэгчид сул шифрлэлтийн төрлийг ашиглах өндөр магадлалтай бөгөөд олноор нь мөрдөн тандах болон цахим гэмт хэргийн хохирогч болох боломжтой гэсэн үг юм. Тиймээс компаниуд төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэх нь энэ төрлийн үйлчилгээ ашигладаг хэрэглэгчдийн эрхийг аливаа заналхийллээс хамгаалаж чадна.

Компаниуд төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэхгүй байх хэд хэдэн шалтгаан бий. Үүнд тодорхой бүтээгдэхүүн, үйлчилгээний шинж чанар, бизнесийн загвар зэрэг багтана. Технологийн олон компаниуд ашиг орлогын нэн тэргүүний эх үүсвэр болох зар сурталчилгаанд ихээхэн ач холбогдол өгдөг бөгөөд тодорхой хэрэглэгчдэд зар сурталчилгаагаа хүргэхийн тулд хэрэглэгчдийн харилцан ярианы агуулгыг унших шаардлага гардаг. Аюулгүй байдал болон бодлогын мэргэжилтнүүдийн бүлэг дурдахдаа" төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлснээр хэрэглэгчдийн мэдээллийн урсгал компаний зар сурталчилгааны загвартай зөрчилдөж, ашиг орлого нь бууруулах магадлалтай"[41] гэжээ. Цаашлаад хэд хэдэн компаниуд харилцан ярианы агуулгыг унших боломжийг олгох зохиомол мэдээллийн үйлчилгээг шуурхай зурвасын үйлчилгээнд нэвтрүүлсэн байдаг.[42]

Төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэхээс зайлсхийх бизнесийн ямар ч үйлдэл нь шуурхай зурвасын үйлчилгээний хэрэглэгчдийн хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөний эсрэг эрсдлээс урьдчилан сэргийлэх арга хэмжээ авч чадахгүй.

Түүнчлэн зарим компаниуд хувьд шуурхай зурвасын үйлчилгээндээ төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэхгүй байх хууль ёсны техникийн шалтгаанаа илтгэдэг. Тухайлбал, хэрэв зурвасын үйлчилгээ нь одоогийн хууль эрх зүйн тогтолцоонд аль хэдийнээ хэрэгжээд эхэлсэн тохиолдолд, ялангуяа Фэйсбүүк (Facebook) Мессенжэрийг веб хөтөчөөр дамжуулан ашиглаж байгаа үед төгсгөл хоорондын шифрлэлтийг хэрэгжүүлэхэд бэрхшээл үүснэ.[43] Нууц үг тайлагч мэргэжилтэн Маттью Грийн хэлэхдээ: "Хэрэв та веб хөтөчөөр дамжин [Facebook] Мессенжэрийг ашигласан тохиолдолд шифрлэлтийн найдвартай байдлыг олж авч чадахгүй." Түүнчлэн шуурхай зурвасын хэрэглэгчид компьютер, таблет, гар утас зэрэг өөр өөр төхөөрөмжинд яг адилхан зурвасыг уншиж хэвшсэн байдаг. Энэ төрлийн үйлчилгээнд төгсгөл хоорондын шифрлэлтийг хэрэгжүүлэх нь хүндрэлтэй ч, тийм ч боломжгүй зүйл биш юм.[44] Энэ тохиолдолд компаниуд техникийн асуудлаа шийдэх хүртлээ эхний алхам болгож төгсгөл хоорондын шифрлэлтийг сонголт болгон оруулж өгөх нь зүйтэй.[45]

Шуурхай зурвасын үйлчилгээ үзүүлэгч компаниуд техникийн асуудалтай тулгараагүй л бол төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэх ёстой гэж Эмнести Интернэшнл үздэг. Компаниуд асуудлыг шийдвэрлэх арга хэмжээг авч, мөн төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэх ёстой. Түүнчлэн тэд өөрсдийн хүсэл эрмэлзлэлийг тодорхой тусгах шаардлагатай юм.

ИЛ ТОД БАЙДАЛ

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Шуурхай зурвасын үйлчилгээ үзүүлэгч компаниуд өөрсдийн хэрэглэгчиддээ тэдний эрх хэрхэн эрсдэлд орж болох тухай мэдээлэх ёстой. Түүнчлэн хэрэглэгчиддээ ямар түвшний шифрлэлтийг санал болгож байгаагаа ил тод байлгаж хэрэглэгчиддээ төгсгөл хоорондын шифрлэлт шиг хүчирхэг шифрлэлтийг санал болгосноо мөн хамгаалалт сул шифрлэлт нь хувийн нууцлалд илүү эрсдэл авчирч болохыг анхааруулсан санамж өгөх ёстой.

---

[41] J.L. Zittrain, M.G. Olsen, D. O'Brien, and B. Schneier, Don't Panic: Making progress on the "Going Dark" debate, Berkman Center for Internet & Society, 1 February 2016, p. 11, available at: https://cyber.harvard.edu/pubrelease/dont-panic/

[42] Tech Crunch, Facebook launches Messenger platform with chatbots, 12 April 2016; Wired, Google's New Allo messaging app gets its edge from AI, 18 May 2016.

[43] Email correspondence with Matthew Green, August 2016.

[44] Motherboard, Why it's harder to encrypt Facebook Messenger than WhatsApp, 8 July 2016.

[45] Email correspondence with Matthew Green, August 2016.

Технологийн компаниуд хүний эрхийг хамгаалах зохих ёсны арга хэмжээг авч байгаагаа харуулахын тулд юуны өмнө хэрэглэгчдийнхээ хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөнд учрах эрсдэл, тэрхүү эрсдлийг бууруулах (шифрлэлтийг ашиглах гэх мэт) арга хэмжээ хэрхэн авч байгаагаа ил тод мэдээллэх ёстой.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Технологийн компаниуд нь мэдээлэл дамжуулах Засгийн газрын шаардлагатай тулгарсан тохиолдолд ил тод байдлын хамгийн дээд түвшинг хангах ёстой. Хэрэглэгчдийн мэдээллийг олж авах Засгийн газруудын шаардлага олон улсын хүний эрхийн хэм хэмжээг зөрчих эрсдэлтэй тохиолдолд компани хүний эрхийг хүндэтгэхийн тулд бүхнийг хийж, хариу арга хэмжээ авах ёстой.

Технологийн компаниуд Засгийн газрын шаардлагыг ил тод байлгахыг хуулийн дагуу хүлээн зөвшөөрдөг мэдээллийг үргэлж хязгаарладаг. Тухайлбал, АНУ-д хэрэв компаниуд Засгийн газраас тушаал хүлээн авсан тохиолдолд олон нийтэд[46] аль болох өргөн хүрээнд мэдээллийг ил болгох ёстой бөгөөд үүний дотор хүлээн авсан шаардлагын төрөл болон тухайн шаардлагатай компани нь нийцэж байгаа эсэх багтана.

Хамгийн гол нь, тодорхой хувь хүний мэдээллийг олж авах шаардлагыг компаниуд тухайн хүнд мэдэгдэх ёстой. Хэрэглэгчдэд мэдээллэдэггүй, түүнийгээ хэрэгжүүлэх тодорхой нөхцөл бүрдүүлээгүй байдлаа компаниуд засч залруулах ёстой.

Шифрлэлт болон Засгийн газрын "харанхуйн хязгаарт хүрэх" айдсыг тойрсон өнөөгийн маргаанд, технологийн компаниуд улс төрийн болон эрх зүйн дарамт шахалтын улмаас арын хаалга гаргах Загсийн газрын шаардлагыг хүлээн авч болзошгүй байна. Ай Фоне (iPhone) утсанд арын хаалга гаргах Холбооны Мөрдөх Товчооны шаардлага гэх мэт тодорхой бүтээгдэхүүнд уг шаардлага хамаарч байна.[47] Түүнчлэн Засгийн газрын албан тушаалтнууд болон эрх баригчид хууль сахиулах үүднээс шифрлэлтийг тойрон гарах шийдвэр гаргаж байна. Компаниуд өөрсдийн зурвасын үйлчилгээнд арын хаалга гаргахгүй байж олон нийтийн итгэлийг олж авах ёстой.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Хүний эрхийн төлөө хүлээсэн үүргийг биелүүлэхээ компаниуд өөрсдийн үйл ажиллагаатай холбоотой сөрөг нөлөөнөөс урьдчилан сэргийлэх үр дүнтэй арга хэмжээ авах чадамжтайгаа харуулах ёстой. Үүнд компани хүний эрхийн эсрэг аюул заналхийлэлд хариу арга хэмжээ авахад үндсэн ажилчид болон олон нийт хангалттай үнэлэлт дүгнэлт өгөх мэдээллийг ил тод байлгах багтана.

Шуурхай зурвасын үйлчилгээ үзүүлэгч компаний нэн тэргүүний үйл ажиллагаануудын нэг нь үзэл бодлоо илэрхийлэх, хувийн нууцтай байх эрхийн зөрчлийг бууруулахын тулд боловсронгуй шифрлэлтийг ашиглах юм.

Компаниуд өөрсдийн үйлчилгээнд ашиглаж буй шифрлэлтийн тогтолцоог аль болох бүрэн дүүрэн нээлттэй байлгах ёстой. Нээлттэй байлгах нь нууц үг тайлагч мэргэжилтнүүд болон цахим аюулгүй байдлын судлаачдад нарийвчилсан судалгаа хийх, хэрэгжүүлж буй шифрлэлт нь найдвартай эсэхийг тодорхойлох, мөн аюулгүй байдлын сул тал эсхүл устгах ёстой вирусыг илрүүлэх боломжийг олгодог байна.

---

[46] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, section 505, Pub. Law No 107-56, 115 Stat. 272 (2001); Electronic Frontier Foundation, Ruling Unsealed: National Security Letters upheld as constitutional, 21 April 2016, available at: www.eff.org/press/releases/ruling-unsealed-national-security-letters-upheld-constitutional

[47] Apple, A Message to Our Customers, 16 February 2016, available at: www.apple.com/customer-letter/

Хамгийн наад зах нь компаниуд ашиглаж буй нууц үг тайлах алгоритм болон протокол зэрэг техникийн тодорхойлолт, мөн түлхүүрүүдийг боловсруулах, солилцох үйл явцын мэдээллийг нийтэлж байх ёстой. Гэхдээ ашиглаж буй шифрлэлтийн аюулгүй байдал болон найдвартай ажиллагааны баталгааг бүрэн дүүрэн хангахад, шифрлэлтийн нээлттэй эхийн протоколыг ашиглах ёстой. Энэ нь шифрлэлттэй холбоотойгоор программын эх кодлолын бүрэлдэхүүн хэсгүүдийг олон нийтэд нээлттэй болгодог гэсэн үг юм. Нээлттэй эхийн протоколыг ашигласнаар шифрлэлтийг хэрхэн хэрэгжүүлэхтэй холбоотой гуравдагч талын аудитыг хийх боломж бүрдүүлдэг

Маттью Грийн Эмнести Интернэшнлд хэлэхдээ "нээлттэй эх сурвалжийн шифрлэлт нь ил тод байх талаасаа сайн алхам төдийгүй аюулгүй байдлын талаасаа ч мөн зөв алхам" юм гэжээ.[48]

СИГНАЛ

Сигнал нь ашгийн бус бүлэг болох Нээлттэй Шивнээ Системийг (НШС) хөгжүүлдэг шуурхай зурвасын программ юм. Энэ нь НШС-ыг хөгжүүлдэг нээлттэй эхийн шифрлэлтийн протокол болох Сигнал Протоколыг ашигладаг. Нууц үг тайлагч болон аюулгүй байдлын мэргэжилтнүүд уг протоколыг "найдвартай систем" гэж тодорхойлдог.[49] Эдвард Сноуден хэлэхдээ "уг протокол нь дамжин өнгөрөх мэдээллийг замаас нь барих үйлдлээс таны зурвасын агуулгыг найдвартай хамгаалдаг" гэжээ.[50] Фэйсбүүк (Facebook), ВатсАпп (WhatsApp), Гүүгл (Google) зэрэг үндсэн шуурхай зурвасын үйлчилгээ үзүүлэгчид өөрсдийн хэрэгжүүлж буй төгсгөл хоорондын шифрлэлтэнд Сигнал Протоколыг ашигладаг гэдгээ баталжээ. 2016 оны 9-р сард, Хилари Клинтоны ерөнхийлөгчийн сонгуулийн сурталчилгааны баг текстэн зурвасын Сигнал программыг ашиглаж байсан нь илэрчээ.[51]

[48] Email correspondence with cryptographer and cybersecurity specialist Matthew Green, Assistant Professor at Johns Hopkins Information Security Institute, August 2016.
[49] Email correspondence with Matthew Green, August 2016.
[50] The Daily Dot, Edward Snowden tells you what encrypted messaging apps you should use, 6 March 2016.
[51] The Financial Times, Hillary Clinton adopts start-up's encryption app, 4 September 2016.

4. КОМПАНИЙ ЖАГСААЛТ

Эмнести Интернэшнл олон нийтэд ил тод компаний мэдээллийг судлаж, мөн Эмнестигийн хүссэн мэдээлэлд хариу өгсөн эсэхийг харгалзан үзэж 11 компаний жагсаалтыг гаргаж, компани тус бүрийг доорх хүснэгтэнд дүгнэж, дэлгэрэнгүй үнэлгээг хавсралт хуудсанд тусгалаа.

Нийт үнэлгээ

Бүх компаниуд өөрсдийн зурвасын программдаа энгийн шифрлэлтийн ерөнхий хэлбэрийг хэрэгжүүлдэг. Гэсэн ч Эмнестигийн гаргасан үнэлгээгээр төгсгөл хоорондын шифрлэлт хамгийн шилдэг сонголт гэдэг нь илт харагдаж байна. Майкрософт, Снапчат, Тенсэнт компаниуд өөрсдийн шуурхай зурвасын үйлчилгээний хэрэглэгчдэд төгсгөл хоорондын шифрлэлтийн ямар ч хэлбэрийг санал болгодоггүй байна.

Гэвч шифрлэлтийг автоматаар хэрэгжүүлдэг гуравхан компани бий. Ихэнх компаниуд шифрлэлтийг хэрэгжүүлдэг талаарх техникийн бүрэн мэдээллийг нууцалдаг нь аюулгүй байдлын мэргэжилнүүдийн хувьд тухайн шифрлэлт найдвартай гэсэн баталгаа өгөхөд илүү хүндрэл учруулж байна. Нэг ч компани өөрсдийн шуурхай зурвасын үйлчилгээнд төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэхдээ нээлттэй эх сурвалжийн шифрлэлтийн протокол ашигладаггүй. Энэ нь шуурхай зурвасын үйлчилгээнд хэрэгжүүлэх шифрлэлтийн тогтолцооны хувьд хамгийн энгийн шаардлага гэж Эмнести Интернэшнл үздэг. Харин Фэйсбүүкийн ВатсАпп нь уг хоёр шаардлагыг хангадаг байна.

Бүх компаниуд хувийн нууцлалын тогтсон үзэл баримтлалтай. Эдгээрийн зарим нь хувийн нууцлалд ноцтой эрсдэл учруулах Засгийн газрын үйлчилгээний аюулгүй байдлыг хязгаарлах саналтай холбоотой шифрлэлтийг тойрсон одоогийн маргааны тэргүүнд байна. Гэвч Айпл(Apple) шифрлэлтэнд арын хаалга гаргах төрийн байгууллагуудын оролдлогыг эсэргүүцэхэд хамгийн бодитой алхам хийж, бусад компани Айпл(Apple)-ын байрь суурийг дэмжих эсхүл нууцлал болон аюулгүй байдлын ач холбогдлын талаар олон нийтэд дуу хоолойгоо өргөж байна.[52]

Майкрософт зэрэг таван компаний хувийн нууцлал, хүний эрхэд заналхийлж буйг тогтоох нь сул, өөрсдийн шуурхай зурвасын үйлчилгээнд хэрэгжүүлэх шифрлэлтийн түвшний үзэл баримтлал нь хоорондоо зөрүүтэй, тэдгээрийн ихэнх нь үзэл бодлоо илэрхийлэх эрх чөлөөний тогтсон үзэл баримтлалгүй байна.

Нийт 11 компаний найм нь эдгээр ноцтой асуудалтай холбоотойгоор мэдээлэл хүссэн Эмнести Интернэшнлийн захидалд хариу өгчээ. Блэйкбэрри, Гүүгл, Тенсэнт компани хариу өгөөгүйд Эмнести Интернэшнл сэтгэл дундуур байна.

Маш цөөн компани нь өөрсдийн зурвасын программуудыг хэрэглэгчдэд хэрэгжүүлж буй шифрлэлтийн түвшний талаарх зохих мэдээлэл өгдөг.

[52] Amicus Briefs in Support of Apple, available on Apple's website at: www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html

ВатсАпп (WhatsApp) нь өөрсдийн харилцаа холбоонд төгсгөл хоорондын шифрлэлтийг хэрэгжүүлээгүй хэрэглэгчдэд сэрэмжлүүлэг өгдөг цорын ганц программ юм. Төгсгөл хоорондын шифрлэлтийг сонголт хэлбэрээр санал болгодог Фэйсбүүк Мессенжэр (Facebook Messenger), Гүүглийн Алло (Google's Alio), КакаоТок (KakaoTalk), Телеграм (Telegram), АйМессэж (iMessage) зэрэг программууд нь аюулгүй байдлын түвшингүүдийн хоорондын ялгаа, сул хамгаалалт, шифрлэлт хүмүүсийн эрхэд өндөр эрсдэл учруулах магадлалтай талаарх мэдээллээ хэрэглэгчдэд бүрэн дүүрэн ойлгуулдаггүй байна.

Судалгаанд хамрагдсан компаниудын хагас нь хэрэглэгчдийн хувийн мэдээллийг авах Засгийн газрын хэд хэдэн шаардлагыг олон нийтэд илчилсэн. Өнөөдөр АНУ-д буй бүх компаниуд АНУ-ын ПРИЗМ хяналтын хөтөлбөрүүдэд корпорациудын хүлээсэн үүргийн талаар илчилсэн Сноудены мэдээлэлд үндэслэн эдгээрийг ил тод мэдээлж байна. Гэвч Засгийн газрын хяналт нь АНУ-ын санаа зовнисон асуудалтай ямар ч хамааралгүй бөгөөд дэлхий дахинд байгаа бүх компаниуд эдгээр шаардлагуудын талаарх мэдээллийг аль болох их хэмжээгээр олон нийтэд ил тод байлгах ёстой.

Тенсэнт компаниас бусад нь өөрсдийн зурвасын үйлчилгээний шифрлэлтэнд арын хаалга гаргах Засгийн газрын шаардлагаг хүлээн зөвшөөрөхгүй гэж олон нийтэд мэдэгджээ.

5. ДҮГНЭЛТ БА ЗӨВЛӨМЖ

Тоон системийн эрин үед шифрлэлт нь хүний эрхийн эсрэг цахим заналхийллээс хамгаалдаг. Энэ нь өөрсдийн ажил хөдөлмөрөөс шалтгаалан эрх бүхий байгууллагын хараа хяналтанд өртөх хүний эрхийн идэвхтнүүдийг хамгаалж, мөн цахим гэмт хэрэг болон хувийн харилцаа холбооны заналхийллээс хүмүүсийг хамгаалахад тусладаг. Шифрлэлт нь хүмүүсийг айдас түгшүүргүйгээр өөрсдийгөө чөлөөтэй илэрхийлж, үзэл бодлоо хуваалцах орон зайг бий болгодог.

Технологийн компаниуд нь хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөнд учрах эсрдлийг бууруулахын тулд шифрлэлтийг хэрэгжүүлэх үүрэг хүлээдэг. Эмнести Интернэшнлийн судалгаанд хамрагдсан технологийн 11 компаниуд нь түүнчлэн шифрлэгдсэн зурвасаар дамжих хэрэглэгчдийн мэдээллийн аюулгүй байдлыг хамгаалахад компаниудын авч буй арга хэмжээ нь хоорондоо ялгаатай байдаг.

Шуурхай зурвасын үйлчилгээнд төгсгөл хоорондын шифрлэлтийг хэрэгжүүлэхгүй байх үндэслэл байхгүй. Одоог хүртэл шифрлэлтийн хамгаалалт султай хэлбэрт найдвар тавьдаг Блэйкбэрри, Майкрософт, Снапчат, Тенсэнт гэх мэт компаниуд өөрсдийн үйлчилгээг ашигладаг сая сая хүмүүсийн хувийн харилцаа холбоог том эрсдэлд оруулдаг. Тэд хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөг хүндэтгэх өөрсдийн үүргийг биелүүлдэггүй.

Бүх компани ил тод байдлаа сайжруулснаар хүмүүс өөрсдийн ашиглаж буй шуурхай зурвасын үйлчилгээнээс ирэх аюул заналхийллээс хэрхэн хамгаалах тухай мэдээллийг бүрэн авах болно.

Технологийн компаниуд хэрэглэгчдийнхээ мэдээллийг төрийн байгууллагуудад дамжуулах дарамт шахалттай тулгарах нь ихэссээр байна. Компаниуд хүн бүрийн хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөнд нөлөөлөх хариу арга хэмжээг хэрхэн сонгох вэ.

Өнөөдөр хувийн нууцлал болон аюулгүй байдлыг дэмжихэд олон нийтийн саналыг авдаг олон компани байдаг. Үүнийг дэмжихэд, мөн хэрэглэгчид, олон нийт, цахим орчинд эдлэх эрх нь аюул заналхийлэл дунд байгаа хүмүүсийн ашиг сонирхолд тулгуурлан өөрсдийн үзэл баримтлалыг харуулахдаа компаниуд хүний эрхийн хандлагыг хүлээн авч байгаа гэдгээ харуулах ёстой.

Шуурхай зурвасын үйлчилгээг үзүүлэгч бүх компаниудад өгөх Эмнестигийн гол гурван зөвлөмж:

1. Шуурхай зурвасын бүх үйлчилгээнд төгсгөл хоорондын шифрлэлтийг автоматаар хэрэгжүүлэх, мөн шифрлэлтэнд хамаарах программын эх кодын бүх хэсгийг нийтлэх.
2. Үйлчилгээнд хэрэгжүүлж буй шифрлэлтийн түвшний талаар өөрсдийн шуурхай зурвасын үйлчилгээний хэрэглэгчдэд тодорхой мэдээлэх.
3. Хуулийн дагуу аль болох дэлгэрэнгүй мэдээлэл бүхий тайланг ил тод тогтмол нийтлэх.

ХАВСРАЛТ: КОМПАНИ ТУС БҮРИЙН ҮНЭЛГЭЭ

АЙПЛ (APPLE)

Айпл нь текст, зураг болон видео хийх зориулалттай апликейшн болох iMessage (Ай Мессэж) ба видео дуудлага хийдэг Facetime (Фэйс Тайм) апп (апликейшн)-аараа дамжуулан шуурхай зурвасын үйлчилгээ (мессенжэр, чат) явуулдаг. Энэ нь хэрэглэгчдэд санал болгож буй асар олон тооны программын төлөөлөл бөгөөд Apple компани нийт 1 тэрбум iPhone утас зарсан хэмээн бодоход өдөр бүр сая сая хүмүүс тус программуудыг хэрэглэдэг гэж тооцож болохоор юм.[53]

Айпл нь хувийн аюулгүй байдал, нууцлалын хүчирхэг дэмжигч бөгөөд өөрийн үйлчилгээндээ өндөр нууцлалтай шифрлэлт ашигладаг. Гэвч Эмнести Интернэшлийн зүгээс Apple хүний эрхийн талаас асуудлуудыг шийдвэрлэхэд үүнээс ч илүүг хийх боломжтой, хэрэглэгчиддээ тэдний хүний эрхэд халдаж буй аюул заналхийлэл, үүнд компани хэрхэн хариу өгч буй талаар мэдэгдэх ёстой гэж үзэж байгаа.

Айпл-ийн зүгээс Эмнести Интернэшнлийн үнэлгээний 2 дахь захидалд хариу өгсөн болно.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Уг шалгуураар Эмнести Интернэшл Apple (Айпл) компанид 2 оноо өгчээ.

Apple (Айпл) компани хувийн нууцлал, мэдээллийн аюулгүй байдлыг хамгаалах тухай онцгойлон заасан амлалт бодлого байдаг ба нууцлалыг хамгаалахын тулд ямар арга хэмжээ авах тухай тусгайлан заасан байдаг. "Хувийн Нууцлалын Бодлого" гэх мэдэгдэлдээ компани нь операторын систем, программ болон тухайн тоног төхөөрөмждөө өндөр хэмжээний сайн хамгаалалт хийх тухай заасан байдаг ба iMessage, FaceTime зэрэг тодорхой нэг үйлчилгээнд хамаарах нууцлалын тухай дурдсан байна.

Технологийн компаниуд Засгийн газрын Цагдан хянах эвсэлтэй хамтран ажилласнаар, Айпл төрөөс мөшгин хянах нь хувийн нууцлал, үзэл бодлоо чөлөөтэй илэрхийлэх эрх, чөлөөнд халдаж байгаа болохыг анзаарч, эдгээр эрхийг хамгаалж баталгаажуулах талаар Засгийн газартай маргаж, хуулийн хамгаалалтыг сайжруулахыг Засгийн газраас шаардсан байна.[54]

Айпл хэрэглэгчдийн хувийн нууцтай байх эрхийг хамгаалахаа амлаж, үүний төлөө мэдээллийн аюулгүй байдал болон хэрхэн ажиллахаа тайлбарласан юм.

[53] The Financial Times, Apple iPhone sales set to pass 1bn milestone, 24 July 2016, available at: www.ft.com/cms/s/0/3e2b61a2-500a-11e6-8172-e39ecd3b86fc.html
[54] Reform Government Surveillance website: www.reformgovernmentsurveillance.com/

Гэвч компаний олон нийтэд нээлттэй бодлогуудад үзэл бодлоо чөлөөтэй илэрхийлэх эрхийг хамгаалах тухай амлалтын тухай заагаагүй байна. Компани нь өөрийн бараа бүтээгдэхүүн болон үйлчилгээнээсээ илүүтэйгээр нийлүүлэлтийн сүлжээндээ хүний эрхийн асуудлаар тусгайлан дурьдсан байдаг ажээ. Иймээс Эмнести Интернэшнл уг шалгуурын хувьд Apple-д хамгийн өндөр оноо өгөх боломжгүй.

Эмнести Интернэшнлийн захидлын хариуд Apple компаний захирал Тим Күк-ийн үг хэлэх эрхийг хамгаалсан мэдэгдлийг дурдсан юм. Жишээ нь, 2016 оны 3 сард хийсэн ярилцлагадаа Күк "Иргэний эрх чөлөөний тухай бодох бүртээ энэ улсыг бий болгосон үндсэн зарчмуудын тухай санадаг. Анхны Үндсэн Хуульд заасан эрх чөлөө болон хувийн нууцтай байх үндсэн эрхийн тухай бодогддог". Тэрээр мөн цааш нь "...өчүүхэн жаахан муу зүйлээс болж сайн сайхан болж байгаа зүйлээ үгүй хийж болохгүй. Заримдаа өөр бусад хүмүүсийн хэлж байгааг сонсоод өмнөөс нь ичих шиг БОЛДОГ үе бий. Гэхдээ бид тэглээ гээд тэдний үг хэлэх эрхийг хааж болохгүй. Энэ бол түүнтэй л адил" гэжээ.[55]

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл уг шалгуурын тухайд Apple (Айпл)-д 3 оноо өгсөн юм.

Apple нь iMessage болон FaceTime программуудын тухайд хэрэглэгчээс хэрэглэгч хоорондын нууцлалыг цаанаас нь өгөгдмөл байдлаар тохируулсан байдаг бөгөөд зарчмын хувьд эдгээр үйлчилгээнд сайн нууцлал хийсэн гэсэн үг. Компани нь өөрөө үйлчлүүлэгчийнхээ захидал харилцааг дундаас нь авч чаддаггүй /нэвтэрч чаддаггүй/ гэж ойлгож болно.

Гэвч iMessage нь мессэжний үйлчилгээнд хийсэн нууцлал "аюулгүй байдлын баталгаа биш" гэдгийг өөрөө харуулдаг. Джонс Хопкинс Их Сургуулийн судлаачдын баг iMessage программын цахим халдлагын эсрэг протоколын аюулгүй байдалд анализ хийсэн ба тэд цахим халдагч iMessage-ийн захидал харилцааг тайлахад ашиглаж болох "эмзэг газруудыг"олжээ.[56] Apple (Айпл) сүүлийн үеийн программ хангамжиндаа эдгээр алдаа дутагдалыг залруулах алхамууд авч эхэлсэн байна. Юутай ч төгсгөл хоорондын нууцлалыг цаанаас нь өгөгдөлөөр тохируулж өгсөн үед ч бодит байдал дээр нууцлалыг хадгалах явцад нууцлал задарч болзошгүй гэдгийг харуулж байна.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Уг шалгуурт 1 оноо өгсөн байна.

Apple (Айпл) нууцлалыг хамгаалах, хэрэглэгчдийнхээ цахим аюулгүй байдлыг хамгаалах байр суууриа олон нийтэд мэдэгдсэн юм. Мөн өөрийн цахим хуудсандаа iMessage ба FaceTime программуудад ашигладаг нууцлалын протокол, мөн захидал харилцааг хэрхэн хамгаалдаг, утас харилцааг чагнах тушаал Apple-д өгсөн ч гэсэн энэ нь боломжгүй тухай тайлбарласан байдаг."

Гэвч компаний зүгээс учирч болох хүний эрхийн эрсдэл, нууцлалын тухай хэрэглэгчдэд мэдээлэл өгөх талаараа хангалттай арга хэмжээ авдаггүй. I Message (Ай Мессэж) стандарт текст мессэжтэй адилхан холболт хэрэглэдэг ба эдгээр нь 2 өнгөөр (ногоон ба цэнхэр) ангилагддаг боловч тэдгээрийн хоорондын аюулгүй байдлын ялгааг хэрэглэгчдэд тайлбарлаж өгдөггүй байна. Стандарт текст мессэжийн программд ямарваа нууцлал байдаггүй учраас ялгаж өгөх нь нэн чухал билээ.

Уг асуудлыг Эмнести Интернэшнлээс тавьсаны дараа Apple iMessage болон SMS-ын хоорондын ялгааг тайлбарласан шинэ зааварчилгааг цахим хуудсандаа нийтлэсэн юм.[57]

---

[55] TIME, Inside Apple CEO Tim Cook's Fight with the FBI, 17 March 2016.
[56] C. Garman, M. Green, G. Kaptchuk, I. Miers, M. Rushanan, John Hopkins University, Dancing on the Lip of the Volcano: Chosen Ciphertext Attacks on Apple iMessage, 2016, (hereinafter: Dancing on the Lip of the Volcano) available at: https://isi.jhu.edu/~mgreen/imessage.pdf
[57] Apple, About iMessage and SMS/MMS, available at: https://support.apple.com/en-us/HT207006

Энэ нь нааштай алхам мөн боловч Apple мессэжийн үйлчилгээн дотроо тодорхой оруулж өгөх нь зүйтэй. I Message болон FaceTime-ийн аль алинд нь ямар түвшний нууцлалын протокол ажиллаж байгаа тухай анхааруулга мөн хүний эрхийн халдагын асуудлыг хэрхэн шийдвэрлэж байгаа тухай ямарваа анхааруулга байддаггүй юм.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Эмнести Интернэшнл Apple-д шалгуурт 3 оноо өгчээ.

Apple-ийн зүгээс Засгийн газраас хүлээн авсан нийт хүсэлтийн тоо бүхий Ил Тод Байдлын Тайланг жилд 2 удаа гаргадаг. Apple (Айпл) Засгийн газрын мэдээллийн хүсэлтэд "бид хуулиар ил болгохыг зөвшөөрсөн мэдээллийг л гаргаж өгдөг" хэмээжээ. Мөн хүсэлтэнд хэрхэн хариулдаг тухайгаа хууль сахиулах хүчнийхэнд зориулсан зааварчилгаандаа нийтлэсэн байна.

Apple Засгийн газруудыг хэрэглэгчийн мэдээллийг авах шаардлагандаа илүү нээлттэй байхыг уриалжээ. 2016 оны 9-р сард тухайн асуудлаар АНУ-ын Засгийн газрын эсрэг Microsoft (Майкрософт)-ын хэрэг дээр Apple тайлбар өгсөн байна. (Microsoft-ийн тухай дараах хэсгээс харна уу).[58]

Компани нь тусгайлан хориглоогүй эсвэл тодорхой нэг онцгой тохиолдлоос бусад үед хэрэглэгчийн хувийн мэдээллийг авах тухай хүсэлт ирвэл хэрэглэгчид мэдэгдэх бодлоготой.

Apple өөрийн нууцлалдаа ямар нэгэн арын хаалга үлдээхгүй байх байр суурийг хатуу баримталдаг. Компаний цахим хуудсанд тавьсан мэдэгдэлдээ: Тим Кук захирал "Бид аль ч улсын ямар ч төрийн агентлагтай хамтран Apple-ын бүтээгдэхүүн болон үйлчилгээнд арын хаалга нууцлалын протоколын араар нэвтрэх нүх сүв гаргаж байгаагүй. Бид мөн хэзээ ч манай сервэрт нэвтрэх зөвшөөрөл олгож байгаагүй. Цаашид ч хэзээ ч ийм зүйлс хийхгүй" гэжээ.[59] Уг байр сууриасаа ухарсан гэх ямарваа баримт, олон нийтийн санал шүүмжлэлийг Эмнести Интернэшнл олоогүй юм. Цаашилбал дээр дурдсанчлан Apple тус байр сууриа шүүхийн өмнө хамгаалж чадсан.

Засгийн газрын хэрэглэгчийн мэдээллийг авах хүсэлтийн тухайд Apple компани нь хангалттай ил тод хэмээн Эмнести үзэж байна.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Эмнести Интернэшнл 1 оноо өгсөн байна.

IOS системийн аюулгүй байдлын зааварчилгаандаа Apple iMessage (Ай Мессэж) болон FaceTime (Фэйстайм) программуудад ашигласан нууцлал техникийн үзүүлэлтийг нийтлэн гаргадаг.[60] Энэ нь түлхүүр үг солих, шинээр авах процессийн талаар товч тайлбарласан боловч эдгээр программ ашигласан нууцлалын протокол нь нээлттэй биш. Джонс Хопкинсийн судлаачдын iMessage программын бичилтэнд хийсэн анализ болон Apple-ийн нууцлалтыг тодорхойлох өмнөх оролдлогуудын үр дүнг харахад "нууцлалын механизмын гол хэсгүүд болон түлхүүр үг бүртгэх ажиллагаа, анхааруулга өгөх механизм бүхэлдээ" орхигдсон хэвээр байна гэж дүгнэжээ. [61] Судлаачид Apple-ийг өөр, илүү нээлттэй протокол ашиглахыг зөвлөсөн байна.

Эмнести Интернэшнлийн захидлын хариуд Apple "бид iMessage болон FaceTime доторх хэрэглэгч хоорондын нууцлал хэрхэн ажилладаг нь манай Аюулгүй Байдлын Бодлогод нээлттэй байдаг" хэмээжээ.

[58] Brief as Amici Curiae by Apple, Lithium Technologies, Mozitta and Twiiio in support of Microsoft Corporation's opposition to defendant's motion to dismiss, 2 September 2016, in Microsoft Corporation v. The United States Department of Justice, case number 2:16-CV-00538, available at: https://blog.mozilla.org/wp-content/uploads/2016/09/Mozilla-Brief-of-Joint-Amicus-in-MSFT-v.-DOJ.pdf
[59] Apple's commitment to your privacy, available at: www.apple.com/uk/privacy/
[60] Apple, iOS Security Guide, pp. 41-42, May 2016, www.apple.com/business/docs/iOS_Security_Guide.pdf
[61] Dancing on the Lip of the Volcano, p. 3.

Блэйкбэрри (BLACKBERRY)

Blackberry нь Канад улсад төвтэй гар утасны үйлдвэрлэгч компани юм. Тус компани нь ухаалаг утасны үйлдвэрлэгч гэдгээрээ олонд танигдсан ба 100 гаруй сая хэрэглэгчтэй мессэжний программ болох Blackberry Messenger (BBM)-ыг программын мөн гаргасан билээ.[62]

Blackberry (Блэйкбэрри)-ын Гүйцэтгэх Захирал Джон Чен нууцлалыг идэвхитэй дэмжсээр ирсэн юм. Тэрээр нууцлалыг хориглох саналуудыг эсэргүүцэж ирсэн боловч нөгөө талаараа компаниуд нь Засгийн газраас тавьж буй "үндэслэл бүхий хууль ёсны нэврэх хүсэлт"-ээс татгалзахгүй байх нь зүйтэй, Blackberry-ийн хувийн нууцлалыг хамгаалах амлалт нь гэмт хэрэгтэнд үйлчлэхгүй хэмээн мэдэгдсэн байна.[63]

Blackberry-ийн зүгээс Эмнести Интернэшнлийн мэдээлэл авах хүсэлтэнд хариу мэдэгдээгүй тул олон нийтэд нээлттэй мэдээллийг хянан судалсаны үндсэн дээр дараах үнэлгээг гаргасан болно.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Эмнести Интернэшнл уг шалгуурын хувьд Блэйкбэрри-д 1 оноо өгсөн юм.

Блэйкбэрри хүний эрхийн бодлоготой бөгөөд үүндээ хувийн нууцлалыг хадгалах компаний зорилтыг тусгасан байдаг. Үүнийг мөн Хувийн Нууцын тухай Бодлогодоо дэлгэрүүлэн тусгажээ.

Гэхдээ компаний хүний эрхийн бодлогод үзэл бодлоо чөлөөтэй илэрхийлэх эрх, эрх чөлөөний тухай тусгагдаагүй байна. Түүнчлэн Блэйкбэрри Засгийн газрын хууль бус хяналтын улмаас хэрэглэгчийн хувийн нууц болон үзэл бодлоо илэрхийлэх эрх чөлөөнд учруулж буй аюул заналхийллийг тодорхой хүлээн зөвшөөрөөгүй юм.

Блэйкбэрри-ийн Хувийн Нууцын тухай Бодлого нь зөвхөн хэрэглэгчийн мэдээллийг хэрхэн хамгаалдаг тухай ерөнхий мэдээллийг агуулсан байдаг ба гагцхүү "Блэйкбэрри нь таны хувийн мэдээлийг хамгаалахын тулд бүтээгдэхүүн, үйлчилгээ, байгууллагын болон техникийн арга хэмжээг сайжруулсан байх болно" гэж бичжээ. Үүнд шифрлэлтийн тухай өгч дурдаагүй байна.

Блэйкбэрри хувийн нууцтай байх эрхыг хамгаалах амлалт өгсөн боловч байгууллагын бодлого нь хэрэглэгчдийн нууцад халдаж буй аюул заналхийлэл болон түүний эсрэг авах арга хэмжээгээ тодорхойлж чадаагүй гэж Эмнести Интерэшнл үзэж байна. Түүнчлэн Блэйкбэрри бүтээгдэхүүн, үйлчилгээ нь хүний эрхэд хэрхэн эрсдэл учруулж буйгаа хүлээн зөвшөөрдөггүй.

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл уг шалгуурын тухайд Блэйкбэрри-д 0 оноо өгөөд байна.

BBM программаар илгээсэн мессэж нь Тээвэрлэлтийн түвшний шифрлэлт ашигладаг ба төгсгөл хоорондын шифрлэлт ашиглах сонголт байдаггүй. Энэ нь компани хэрэглэгчдийн захидал харилцаанд нэвтрэх боломжтой гэсэн үг юм.

Блэйкбэрри хамгаалалт бүхий шуурхай зурвас явуулах "BBM Protected" гэх үйлчилгээг мөн үзүүлдэг ба үүнд төгсгөл хоорондын шифрлэлтийг ашиглажээ. Гэхдээ энэ нь Блэйкбэрри-ийн Корпорацуудад зориулан төлбөртэй үйлчилгээ юм.[64] BBM программын энгийн хэрэглэгч уг үйлчилгээг авах өөр боломж байдаггүй. Блэйкбэрри захидал харилцааг илүү нууцлах шаардалагатай гэдгийг хүлээн зөвшөөрч байгаа нь үүнээс харагдаж байгаа ба хэрэглэгчдийнхээ төлбөрийн чадвараас хамааран өөр өөр түвшний хамгаалалт санал болгож буй нь дутагдалтай байна.

---

[62] Statists, Leading social networks worldwide as of September 2016, ranked by number of active users, September 2016, available at: www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
[63] J. Chen, Executive Chairman and CEO of Blackberry, The Encryption Debate: a Way Forward, 15 December 2015, (The Encryption Debate: a Way Forward) available at: http://blogs.blackberry.com/2015/12/the-encryption-debate-a-way-forward/
[64] Blackberry, Overview of BBM Protected, available at: http://support.blackberry.com/kb/articleDetail?ArticleNumber=000035648)

Блэйкбэрри өөрийн BBM программын энгийн хэрэглэгчдийн эрхийг хүндэтгэх үүргээ биелүүлэхгүй байна гэж Эмнести дүгнэлээ.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Тус шалгуурын хувьд Блэйкбэрри-д 1 оноо өгсөн болно.

Хэрэглэгчдэд туслах цахим хуудсандаа Блэйкбэрри BBM болон BBM Protected нь мессэжийг хэрхэн хамгаалдаг, эдгээр программуудад ямар төрлийн шифрлэлт ашигладаг тухайгаа тайлбарлажээ.[65]

Гэхдээ, компани хэрэглэгчддээ эдгээр шуурхай зурвасын үйлчилгээг ашиглах үед тэдний хүний эрх хэрхэн эрсдэл орж болох тухай мэдээллийг өөрийн цахим хуудас болон үйлчилгээнд нэвтрэх үед мэдэгддэггүй.

BBM программ дотор, хэрэглэгчдэд тэдний хувийн мэдээлэл, хүний эрхэд учирч болох эрсдэл эсвэл үйлчилгээнд ашиглагдаж буй шифрлэлтийн түвшний тухай мэдээлэл байдаггүй. Өөрөөр хэлбэл хэрэглэгчид Блэйкбэрри тэдний захидал харилцааг хэрхэн хамгаалж байгаа тухай ямар ч ойлголт байхгүй гэсэн үг.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Эмнести Интернэшнл тус шалгуурын тухайд Блэйкбэрри-д 0 оноо өгөв.

Хэрэглэгчдийн мэдээллийг олж авах гэсэн Засгийн газрын хэдэн хүсэлт хүлээн авсан тухайгаа Блэйкбэрри ил болгодоггүй. Блэйкбэрри-ийн хэвлэл мэдээллийн төлөөлөгч компаний зүгээс ойрын ирээдүйд ил тод байдлын тайлан гаргах төлөвлөгөөгүй байгаа тухай олон нийтэд мэдэгдсэн юм.[66]

Блэйкбэрри компаний Гүйцэтгэх захирал "Блэйкбэрри өөрийн бүтээгдэхүүн болон программдаа "арын хаалга" гаргахаас татгалздаг. Бид хэзээ ч Засгийн газрын өөрийн сервэртээ нэвтрүүлж байгаагүй ба цаашдаа ч нэвтрүүлэхгүй" хэмээн ил тод мэдэгдсэн байна.[67] 2015 оны 11 сард Пакистан улсын Засгийн газар тэдний сервэрт нэвтрэхийг шаардсаны дараа Пакистан дахь үйл ажиллагаагаа хаажээ.[68] Уг шийдвэрийг цахим эрхийг дэмжигч бүлгүүд сайшаан хүлээн авсан байна.[69]

Гэвч Блэйкбэрригийн хэрэглэгчийн шуурхай зурвасын үйлчилгээ дундын глобал шифрлэлтийн түлхүүр хэрэглэдэг ба 2016 оны 4 сард Motherboard ба Vice News-ын явуулсан шалгалтаар Блэйкбэрри гэмт хэмгийн мөрдөн байцаалттай холбогдуулан Royal Canadian Mounted Police-д глобал шифрлэлтийн нэвтрэх нууц түлхүүрээ өгсөн болохыг илрүүлжээ.[70] Энэ нь үндсэндээ хууль сахиулах хүчинд "урд хаалга"-аа нээж өгсөнтэй адил бөгөөд BBM-ээр дамжиж буй бүх мэдээллийг авах боломжтой юм.

Энэ тухайд Блэйкбэрригийн Гүйцэтгэх Захирал хэлэхдээ "Блэйкбэрригийн туслалцааны тухайд бид манай хууль ёсны мэдээлэл авах зарчмынхаа байр суурийг хадгалсаар байгаа. Цаашилбал, уг хэрэг явдалд Блэйкбэрригийн БЕС сервэр огт холбогдоогүй" хэмээн мэдэгджээ.

[65] Blackberry, BBM security, available at: http://help.blackberry.com/en/bbm-security; BBM Protected security, available at: http://help.blackberry.com/en/bbm-protected-security
[66] Z. Whittaker, ZDNet, BlackBerry, once a security pioneer, falls behind on privacy, transparency, 19 November 2015, available at: www.zdnet.com/article/blackberry-has-no-plans-for-locking-out-feds-from-data-demands/
[67] The Encryption Debate: a Way Forward.
[68] M. Beard, Chief Operating Officer, Blackberry, Why BlackBerry is Exiting Pakistan, 30 November 2015, available at: http://blogs.blackberry.com/2015/ll/why-blackberry-is-exiting-pakistan/
[69] "Access Now and 10 other NGOs, Open letter to BlackBerry on rejecting backdoors and protecting human rights, 22 December 2015, available at: https://www.accessnow.org/13354-2/
[70] J. LingandJ.Pearson, Vice News and Motherboard, How Canadian Police Intercept and Read Encrypted BlackBerry Messages, 14 April 2016, available at: http://motherboard.vice.com/read/rcmp-blackberry-project-clemenza-global-encryption-key-canada

Манай БЕС халдашгүй хэвээр байгаа, арын хаалгын оролт мөн байхгүй төдийгүй бүх гар утасны төхөөрөмжийн хамгийн аюулгүй хамгаалалттай флатформ юм."[71] Гүйцэтгэх Захирал BBM-ын хэрэглэгчдийн сервэрийн тухай огт дурдаагүй билээ. Компаний "хууль ёсны мэдээлэл авах зарчим" нь зөвхөн хэн нэгэн хувь хүн эсвэл дансны мэдээллийг өгч, бусад нийт захидал харилцаанд нэвтрэхгүй гэх баталгаа болохгүй.

2008-2013 оны хооронд Блэйкбэрри компани Энэтхэгийн Засгийн газартай хууль сахиулах хүчнийхэн үйлчилгээнд нь нэвтрэх асуудлаар томоохон маргаантай байсан билээ. Блэйкбэрри эцэст нь Энэтхэгийн Засгийн газарт корпорацийн үйлчилгээний сервэрт нэвтрүүлэхээс татгалзсан боловч BBM зэрэг хэрэглэгчийн үйлчилгээндээ зохих хэмжээний "хууль ёсны нэвтрэх шийдэл" гаргаж өгсөн болохоо мэдэгджээ.[72] Энэ нь чухамдаа юуг хэлж байгаа мөн Энэтхэгийн эрх баригчдад шифрлэлтийн түлхүүрийг өгсөн эсэх нь тодорхойгүй байна.

Блэйкбэрри нь хэрэглэгчдийн мэдээллийг авах гэсэн Засгийн газрын хүсэлтэд хэрхэн хариулдаг нь ил тод бус хэмээн Эмнести Интернэшнл дүгнээд байна. Шифрлэлтдээ "арын хаалга"-ны орох эрх олгодоггүй гэж мэдэгдсэн нь магтууштай боловч уг мэдэгдлээ бодитоор хэрэгжүүлэхгүй байгаа тохиолдлууд байсаар...

Хэрвээ компани шифрлэсэн захидал харилцаанд нэвтрэх эрхийг төрийн байгууллагад өгсөн бол энэ нь хэрэглэгчдийн хувийн нууцад зохисгүй халдсан явдал гарцаагүй мөн.

Аль ч тохиолдолд Блэйкбэрри корпорацийн үйлчилгээний аюулгүй байдлыг сайтар хангадаг болохыг баталж байгаа боловч энгийн үйлчилгээ авч буй хэрэглэгчидээ хэрхэн хамгаалдаг тухайгаа баталж чадахгүй байна. Эмнести Интернэшнлийн зүгээс эдгээр асуудал дээр тайлбар өгөх боломжийг Блэйкбэрри-д олгосон боловч тус хэвлэлийг гаргах хүртэл хугацаанд Блэйкбэрри хариу өгөөгүй билээ.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Уг шалгуурын хувьд Блэйкбэрри-д 1 оноо өгөөд байна.

Блэйкбэрри нь BBM болон BBM Protected үйлчилгээнд ашигладаг шифрлэлтийн тухай дэлгэрэнгүйг Аюулгүй Байдлын тухай бодлогоороо дамжуулан хэвлэн гаргадаг боловч[73] нээлттэй шифрлэлтийн протокол ашигладаггүй.

FACEBOOK (Фэйс Бүүк)

АНУ-д төвтэй мэдээллийн хэрэгслийн компани болох Фэйсбүүк нь 2 шуурхай зурвасын үйлчилгээ явуулдаг ба эдгээр нь яг одоо дэлхийд хамгийн олон хэрэглэгчтэй буюу 1 тэрбум идэвхитэй хэрэглэгч бүхий Фэйсбүүк Мессенжэр болон ВатсАпп (WhatsApp) юм.[74]

Фэйсбүүк нь Эмнести Интернэшнлийн мэдээлэл авах хүсэлтэнд хариулсан болно.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Уг шалгуурын тухайд Фейсбүүк-т 2 оноо өгөөд байна.

[71] J. Chen, Lawful Access, Corporate Citizenship and Doing What's Right, 18 April 2016, available at: http://blogs.blackberry.eom/2016/04/lawful-access-corporate-dtizenship-and-doing-whats-right/#disqus_thread
[72] Reuters, RIM: BlackBerry security not compromised in India, 2 August 2012, available at: http://in.reuters.com/article/rim-india-blackberry-idINDEE87101A20120802
[73] Blackberry, BBM Protected Security Note, June 2016; BBM Security Note, May 2015.
[74] Facebook, Thank You Messenger, 20 July 2016; WhatsApp, One Billion, 1 February 2016.

Фэйсбүүк нь өөрийн Глобал Сүлжээний Санаачлага (GNI)-д нэгдсэн хүний хувийн нууц, үзэл бодлоо чөлөөтэй илэрхийлэх эрх чөлөөг хамгаалахаа мөн[75] "хэрэглэгчдийн хувийн нууцтай байх эрхийг хамгаалахын тулд үйл ажиллагаа явуулж буй улс орон бүрийнхээ эрхийг хамгаалах"-д амласан байдаг. Фэйсбүүкийн "Нууцлалын тухай анхан шатны мэдлэг" хэсэгт хувийн мэдээллийг хамгаалах үүдээс Фэйсбүүк ямар арга хэмжээ авдаг (шифрлэлт гэх мэт) тухай бичсэн байдаг.

Технологийн компаниудын Засгийн Газрын Хяналтын Өөрчлөлт эвслийн гишүүнчлэлээрээ дамжуулан Засгийн газрын хууль бус хяналт хүний эрхэд халдаж байгааг хүлээн зөвшөөрчээ.

Дэлхийн Сүлжээ Санаачлагаар дамжуулан Фэйсбүүк нь компаний холбогдох дотоод систем, бодлого, процедуртаа хөндлөнгийн үнэлгээ тогтмол хийлгэдэг. Фэйсбүүкийн эхний үнэлгээг 2016 оны 7 сард хэвлэн гаргасан бөгөөд "Фэйсбүүк нь өөрийн өдөр тутмын үйл ажиллагаандаа Дэлхийн Сүлжээ Санаачлагын зарчмыг хэрэгжүүлэх бодлого, процедур боловсруулан гаргасан" бөгөөд компани нь дээрх зарчмыг хүндэтгэн дагаж мөрддөг болохыг тогтоожээ.[76]

Гэвч Дэлхийн Сүлжээ Санаачлагын үнэлгээний процесс нь нээлттэй бус учраас Эмнести Интернэшнл дүгнэлтийг баталгаажуулж чадаагүй. Фейсбүүкийн олон нийтэд нээлттэй бодлогод хувийн мэдээллийг нууцлах тухай амлалт тусгагдсан. Иймээс Эмнести Интернэшнл Блэйкбэрри-д 2 оноо өгөөд байна.

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Уг шалгуурын тухайд Блэйкбэрри-д 2 оноо өгөөд байна.

Фэйсбүүкийн Мессенжэр болон ВатсАпп үйлчилгээнд өөр өөр түвшний шифрлэлтийг ашигладаг.

2016 оны 4 сард ВатсАпп текст мессэж, зураг, видео болон дуудлага хийх зэрэгтээ төгсгөлийн шифрлэлт нэвтрүүлэх болсноо мэдэгдсэн юм.[77] ВатсАпп мөн төгсгөлийн шифрлэлтийг автомат болгож өгсөн ба хэрэглэгч программын хамгийн сүүлийн үеийн хувилбарыг хэрэглэж байгаа тохиолдолд бүх харилцаа холбоонд шууд автоматаар ашиглагддаг байна. Уг апликейшн асар олон тооны хэрэглэгчтэй учраас цахим аюулгүй байдлыг сайжруулахад чухал алхам боллоо хэмээн хувийн нууцтай байх эрхийг дэмжигчид таалан хүлээн авсан.[78]

Үүний дараа Фэйсбүүк Мессенжэр апликейшн дээрээ төгсгөл хоорондын шифрлэлтийг ашиглахаар туршиж буй тухайгаа мэдэгдсэн юм.[79] Гэхдээ ВатсАпп-аас ялгаатай нь Мессенжэр үйлчилгээнд автоматаар ажилладаггүй бөгөөд зөвхөн "Нууц Яриа" (Secret Conversation) сонголтыг хийсний дараа явуулсан мессэж, зурганд төгсгөлийн шифрлэлт хийгддэг байна. Энгийн мессэжийн хувьд Мессенжэр нь нууцлалыг хадгалах үүднээс HTTPS зэрэг аюулгүй харилцааны сувгийг ашигладаг нь Тээвэрлэлтийн (Зөөврийн) Түвшний Шифрлэлт хэрэглэдэг гэсэн үг.[80] Өөрөөр хэлбэл мессэж нь Фэйсбүүк болон хэрэглэгчийн хооронд шифрлэгдсэн байдаг боловч компаний зүгээс шифрлээгүй мэдээлэлд нэвтрэх, агуулгыг үзэх бүрэн боломжтой ажээ.

Мессэнжир аппликэншд төгсгөлийн шифрлэлийг автоматаар бус сонголт байдлаар ашиглахаар оруулсан нь хувийн нууцтай байх эрхийг дэмжигчдээс ихээхэн шүүмжлэл хүлээсэн билээ. Электроник Фронтейр Сангийн ахлах хуульч "Төгсгөлийн шифрлэлийг автоматаар оруулаагүй учраас аюулгүй платформ гэж үзэж болохгүй" гэжээ.[81]

---

[75] The Global Network Initiative (GNI) is a multi-stakeholder group of companies, NGOs, academics and investors set up to address issues of privacy and freedom of expression linked to the ICT sector. GNI participants commit to a set of principles, as well as a governance structure. The GNI has been criticized by some civil society organizations, including Amnesty International. In February 2016, the NYU Center for Business and Fluman Rights resigned its membership, citing concerns including weaknesses in the GNI's accountability mechanisms. In 2013, the Electronic Frontier Foundation resigned from GNI, citing a fundamental breakdown in confidence that the group's corporate members are able to speak freely about their own internal privacy and security systems in the wake of the Snowden revelations. For more information see Global Network Initiative website: http://globalnetworkinitiative.org/
M. Posner and S. Labowitz, NYU Center for Business and Human Rights resigns its membership in the Global Network Initiative, 1 February 2016, available at: http://bhr.stern.nyu.edu/statement/cbhr-letter-of-resignation-gni
EFF, EFF Resigns from Global Network Initiative, 10 October 2016, available at: www.eff.org/press/releases/eff-resigns-global-network-initiative

[76] GNI, Public Report on the 2015/16 independent Company Assessments, pp. 21-22, 7 July 2016.

[77] WhatsApp blog, End-to-end encryption, 5 April 2016, available at: https://blog.whatsapp.com/10000618/end-to-end-encryption

[78] For example, security researcher Kenneth White, Director of the Open Crypto Audit Project, quoted in Threatpost, WhatsApp Encryption A Good Start, But Far From a Security Cure-all, 6 April 2016, available at: https://wp.me/p3AjUX-uuO

[79] Facebook, Messenger starts testing end-to-end encryption with eecret conversations, 8 July 2016.

[80] Facebook letter to Amnesty International, 3 August 2016 (Facebook letter).

[81] Quoted in Buzzfeed, You'll have To Turn On Encryption To Protect Your Facebook Messages, 8 July 2016.

Фэйсбүүкийн зүгээс “Нууц яриа” хэсэг нь зөвхөн илгээгч болон хүлээн авагч төхөөрөмж уг захидал харилцааг унших боломж олгох зорилгоор “Нууц яриа” хэсгийг гаргасан хэмээн мэдэгдсэн юм. Энэ нь хэрэглэгч “Нууц яриа” хэсгийг ашиглан явуулсан мессэж, зурвасаа дараа нь өөр гар утас, таблет эсвэл компьютерээр орж эргэн үзэх боломжгүй[82] бөгөөд “хүн бүрд тохирох” сонголт бий хэмээн компаний зүгээс хэлжээ.[83] Фейсбүүкийн Аюулгүй байдлын ахлах Алекс Стамос “Фейсбүүк Мессенжэр бол олон төхөөрөмж дамжин хэрэглэгддэг апликейшн, тиймээс бид төгсгөлийн шифрлэлтийн хэрэглээ сайжирч олон төхөөрөмж дамжих боломж олгоно гэдэгт найдаж байна” гэв.[84]

Энэ нь төгсгөлийн шифрлэлтийг хэрэглэхгүй байх хангалттай шалтгаан биш. Нууц Яриа болон ВатсАпп апликейшнд ашиглаж буй Сигналь протокол нь олон төхөөрөмж дамжин нэвтрэх боломжтой бөгөөд Нууц Яриа болон ВатсАпп апликейшны аль аль нь өөр төхөөрөмж хэрэглэхийг зөвшөөрдөг. Гэхдээ Стамосийн өгсөн өөр нэгэн шалгаан бол “Олон сая хүн апликейшн биш цахим хуудсаар дамжин Мессенжэр хэрэглэдэг. Утасаар дамжуулахгүйгээр код эсвэл түлхүүрийг баталгаажуулах боломжгүй” гэжээ.[85] Эмнести Интернэшнл техникийн шинжээчдээс уг асуудлаар тодруулга авах үед тэрээр цахим хуудас ашиглах шуурхай захидал, мессэж илгээж байгаа үед төгсгөлийн шифрлэл хийхэд техникийн томоохон асуудал/бэрхшээл тулгарж болохыг батласан юм.[86] Энэ нь Нууц Яриа хэсгийн Фэйсбүүкийн цахим хуудас эсвэл цахим хуудсанд тулгуурласан Мессенжэрт нэгтгэн оруулах ажлыг хүндрэлтэй болгож байгаа бөгөөд Нууц Яриа хэсгийг одоогийн байдлаар зөвхөн утас эсвэл таблетээр ашиглах боломжтой.

Эмнести Интернэшнл олон талыг харгалзан авч үзсэний эцэст уг шалгуур дээр Фейсбүүк-т 2 оноо өгсөн юм. ВатсАпп төгсгөлийн шифрлэлийг автоматаар хэрэгжүүлдэг ба цаашид Фейсбүүк Мессенжэр- ээ мөн төгсгөлийн шифрлэл ашигладаг болгох хэрэгтэй. Төгсгөлийн шифрлэлийг сонголт байдлаар оруулж өгсөн нь гарцаагүй нааштай алхам мөн боловч Фейсбүүк төгсгөлийн шифрлэлийг автоматаар ашиглах амлалтаа зайлшгүй биелүүлэх ёстой бөгөөд гүйцэтгэж дуусах эцсийн цаг хугацааны зорилтоо тогтоох ёстой.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Үүнд Эмнести Интернэшнл 1 оноо өгчээ.

Facebook (Фейсбүүк) хувийн нууцлалын тухай бодлого баримталдаг, Messenger (Мессенжэр) болон Whatsapp (ВатсАпп) дэх шифрлэлтийг ашиглан хэрэглэгчдийн мэдээллийг хэрхэн хамгаалдаг, хэрэглэгчдийн мэдээллийг авах гэсэн Засгийн газрын шаардлагыг хэрхэн шийдвэрлэдэг тухай өөрийн цахим хуудсандаа тодорхой нээлттэй дэлгэдэг.

Апликейшн дотроо ВатсАпп нь хэрэглэгч хоорондоо эсвэл групп дотор явуулсан мессэж нь шифрлэлттэй болохыг сануулсан анхааруулга гарч ирдэг бөгөөд хэрэглэгч аливаа нэг захидал харилцаа нь шифрлэгдсэн эсэхийг шалгах боломжтой. Мөн уг апликейшн нь төгсгөл хоорондын шифрлэлт хийгдээгүй бол анхааруулга өгдөг байна.

Гэхдээ ВатсАпп нь хэрэглэгчдэд мессэжээ онлайн “cloud” (клауд) сервэр хадгалсанаас үүсч болох эрсдэлийн тухай сануулдаггүй. Мессэжний бусад олон үйлчилгээний нэгэн адилаар ВатсАпп нь хэрэгчиддээ чатаар бичсэн түүхээ Google Drive (Гүүгл Драяв), iCloud (Ая Клауд) эсвэл тухайн төхөөрөмжинд хадгалах боломжийг санал болгодог. Энэ нь утсаа гээсэн эсвэл хулгайд алдсан үед өмнөх мессэжээ сэргээх боломжийг олгодог учраас олон хүний хувьд маш хэрэгцээтэй үйлчилгээ билээ. Гэхдээ ийм төрлийн мессэж нь эцсийн хэрэглэгч дээр очоод тайлагдах биш, тайлагдсан мессэж хэлбэрээр цахим сервэрт хадгалагддаг учраас утасны системийг сэргээн суулгах үед нууцлалаа алдах боломжтой. Цахим сервэрийн үйлчилгээ олгож буй байгууллага мөн мэдээллийг задлах эрсдэлтэй. ВатсАпп дээр гарч ирдэг анхааруулганд уг онцлогын тухай гардаггүй.

---

[82] Facebook letter.
[83] Facebook letter.
[84] Tweet by Alex Stamos, 8 July 2016, available at: https://twitter.com/alexstamos/status/751416166032117760
[85] Tweet by Alex Stamos, 8 July 2016, available at: https://twitter.com/alexstamos/status/751416491317161984
[86] Email correspondence with cryptographer and cyber-security specialist Matthew Green, Assistant Professor at Johns Hopkins Information Security Institute, August 2016.

Мессенжэрт хэрэглэгчдэд ээлтэй олон арга хэрэгсэл, Фейсбүүкийн Мэдээллийн Сангийн Бодлого болон мэдээллийг олж авахыг хүссэн хууль ёсны өргөдөлд хэрхэн хариулдаг тухай холбоос байдаг. Шинэ зурвас бичих тохиолдол бүрт secret conversation "нууц яриа" хийх эсэх талаар асуулт гарч ирдэг ба цоожны зурагтай байдгаараа энгийн мессэжний хэсгээс ялгардаг. Гэвч Мессенжэр энгийн яриа, мессэж рүү шилжиж байгаа хэрэглэгчдэд "энэ нь илүү сул түвшний хамгаалалт бөгөөд хэрэглэгчдийн мэдээллийн аюулгүй байдал, хүний эрх эрсдэлд" орж болзошгүй талаар анхааруулга өгдөггүй.

Фейсбүүк хэрэглэгчиддээ тэдний хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөө нь эрсдэлд орж буй тухай мэдэгдэх тал дээр илүү ихийг хийх ёстой. Хэдийгээр Фейсфүүк Засгийн газрын хууль бус хяналт нь хүний эрх, эрх чөлөөд халдаж байгаа гэдгийг хүлээн зөвшөөрсөн боловч энэ тухайгаа ВатсАпп үйлчилгээний цахим хуудсандаа дурдаагүй байна. Мөн компаний цахим хуудас болон апликейшнийхээ мэдээллийн хэсгийн аль алинд олон улсын хүлээн зөвшөөрөгдсөн хүний эрхийн хэм хэмжээг биелүүлэх тухай тодорхой заагаагүй байна.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Эмнести Интернэшл тус шалгуурын тухайд Фейсбүүк компанид 3 оноо өгсөн.

Фэйсбүүк Глобал Ил Тод Байдлын Тайландаа Засгийн газруудаас хүлээн авсан хэрэглэгчийн мэдээллийг задлах хүсэлтийн тоог улс улсаар нь тооцоолон гаргадаг. Уг тоо нь Фейсбүүкийн Мессенжэр болон ВатсАпп зэрэг бүтээгдэхүүн үйлчилгээтэй холбоотой тоо бөгөөд зарим нэг мэдээллийг гаргасан нийт хүсэлтийн тоог мөн тусгасан байдаг. "Хуулиар хориглоогүй, хүүхдийн мөлжлөг, аюул гамшиг эсвэл урьдчилан анхааруулах нь сөрөг үр нөлөөтэй" зэрэг тохиолдлоос бусад үед хэрэглэгчиддээ мэдээллийг нь задлахаасаа өмнө мэдэгдэх бодлогыг Фейсбүүк баримталдаг[87] ба мөн улс орнууд бүртгэл дансанд ямар нэг байдлаар халдаж байна гэж сэжиглэвэл хэрэглэгчиддээ мэдэгдэнэ гэдгээ цохон тэмдэглэсэн байна.[88]

Фейсбүүк мэдээлэл авахыг хүссэн хууль сахиулах хүчний ажилчдад зааварчилгаа өгдөг бөгөөд хүсэлт бүр нь "холбогдох хууль тогтоомжтой нийцэж буй эсэх, шүүхийн харьяалал болон олон улсаар дагаж мөрддөг хэм хэмжээнд нийцэж буй эсэхийг" манай хамт олон нарийн нягтлан шалгадаг гэв.

Эмнести Интернэшнлд өгсөн хариундаа "Бид системдээ арын хаалга хийдэггүй" хэмээн мэдэгдсэн юм.[89] Дээр өгүүлсэнчлэн ВатсАпп нь Бразилийн эрх баригчид болон АНУ-ын Холбооны Мөрдөх Товчоо зэрэг хууль сахиулах хүчнийхэнтэй маргаантай байдаг нь улсууд уг үйлчилгээнд нэвтрэх онцгой эрхгүй гэдгийг харуулж байна.[90] Эдгээр хэргийн тухайд Фейсбүүк хувийн нууцыг хамгаалах бодлогоо зөрчсөн гэх ямарваа нотолгоо эсвэл олон нийтийн гомдол байхгүй байна.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Эмнести Интернэшнл энэ шалгуурт 3 оноо өгчээ.

Мессенжэрийн "Нууц Яриа" болон ВатсАпп хоёулаа Нээлттэй Шивнээ системийг хэрэглэдэг бөгөөд энэ олон нийтэд нээлттэй систем төдийгүй крипто нууцлалын мэргэжлэлтүүд нягт судалсан систем юм. Фейсбүүк тус 2 апликейшнд мөн хэрхэн припто хийдэг тухай техникийн тайлбар бүхий илтгэлээ хэвлэн гаргасан байдаг.[91]

Мессенжэрээр явуулдаг энгийн шуурхай захиа, дуудлага (Нууц яриа биш гэсэн үг) нь өөр шифрлэлтийн протокол хэрэглэдэг.

[87] Facebook, Information for law enforcement authorities, available at: https://en-gb.facebook.com/safety/groups/law/guidelines/
[88] Facebook letter.
[89] Facebook letter.
[90] The New York Times, WhatsApp encryption said to stymie wiretap order, 12 March 2016, available at: www.nytimes.com/2016/03/13/us/politics/whatsa pp-encryption-said-to-stymie-wiretap-order.html
[91] WhatsApp, Encryption Overview: Technical Whitepaper, 4 April 2016; Facebook, Messenger Secret Conversations: Technical Whitepaper, 8 July 2016.

Мессенжэр апликейшны хувьд MQTT протокол-ыг ашигладаг байна.[92] Цахим хуудсаар дамжуулан илгээсэн мессэжүүд нь нь автоматаар FITTPS прокотол ашиглан илгээгддэг.[93]

GOOGLE (ГҮҮГЛ)

Саяхныг хүртэл АНУ-д төвтэй интернэт үйлчилгээний Google (Гүүгл) компаний үндсэн мессэжний үйлчилгээ нь Гүүгл Hang Outs (Хэнг-Аутс) байсан юм. Хэнг-Аутс нь цахим хуудсаараа болон өөрийн апликейшнээрээ дамжуулан шуурхай зурвас явуулах, дуут болон видео бичлэг хийх зэрэг боломжийг хэрэглэгчдэд олгодог. Гэвч Гүүгл саяхан шинээр 2 Мессенжэр апликейшн-Allo (Алло) буюу зурвас, зураг видео солилцох мөн видео дуудлага хийх Duo (Дуо) апликейшн зэргийг 2016 оны 8 болон 9 саруудад тус тус гаргажээ.

Гүүгл Хэнг-Аутс хэрэглэгчдийн статистик мэдээллийг гаргаагүй боловч ажиглагчид 2 тэрбум илүү хэрэглэгчидтэй хэмээн тооцоолжээ.[94] Android (Андройд) утас хэрэглэгчид Дуо-г албан ёсоор хэрэглээнд нэвтэрсэнээс нь хойш долоо хоногийн хугацаанд 5 саяаас илүү удаа татан суулгасан байна.[95]

Эмнести Интернэшнл шифрлэлтийн асуудлаар Гүүгл-д хандсан боловч Гүүглийн зүгээс Эмнести Интернэшнлийн захидалд хариу мэдэгдээгүй тул манай уг үнэлгээ нь Гүүглийн олон нийтэд нээлттэй байдаг эх сурвалжуудад тулгуурлан хийсэн үнэлгээ болно.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Уг шалгуурт Гүүгл компанид 2 оноо өгөөд байна.

Фейсбүүк, Microsoft (Майкрософттой) нэгэн адилаар Гүүгл нь Глобал Сүлжээний Санаачлагад нэгдэн хэрэглэгчдийнхээ хувийн нууцтай байх эрх, үзэл бодлоо чөлөөтэй илэрхийлэх эрхийг хамгаалахаа амласан билээ. Компаний зүгээс мөн Технологийн компаниудын Засгийн газрын ажиглалтын эвслийн гишүүнчлэлтээр дамжуулан Засгийн газрын хууль бус хяналт явуулах нь хүний эрхэд халдаж буй хэрэг болохыг хүлээн зөвшөөрчээ. Компаний Нууцлалын тухай Бодлогод шифрлэлт ашиглах зэргээр нууцлалыг хамгаалах үүднээс Гүүглийн авч хэрэгжүүлж буй зарим ажиллагаануудыг жагсаасан байдаг.

Эмнести Интернэшнл компанийхаа бодлого, процедурын дэлгэрэнгүйг хуваалцахыг хүссэн бөгөөд Гүүглийн зүгээс хариу мэдэгдээгүй юм. Гүүглийн олон нийтэд нээлттэй бодлого журманд хувийн нууцлалыг хамгаалах тухай заасан байдаг боловч үзэл бодлоо илэрхийлэх эрх чөлөөг дээдлэх хүндэтгэх тухай дурдаагүй байгаа юм.

Иймд уг шалгуурын хувьд Эмнести Интернэшнл Гүүгл компанид 2 оноо өгөөд байна.

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл үүнд ердөө 1 оноо өгсөн юм.

Гүүгл Хэнг-Аутс нь одоогоор тээвэрлэлтийн шифрлэл хэрэглэдэг, энэ нь төгсгөл хоорондын шифрлэлт хэрэглэдэггүй гэсэн үг ба зөвхөн хэрэглэгч болон Гүүглийн сервэрийн хооронд шифрлэгддэг байна.[96]

Дуо нь бүх видео дуудлагандаа автоматаар төгсгөлийн шифрлэл хэрэглэдэг боловч Аллогийн хувьд төгсгөлийн шифрлэлтийг зөвхөн нэмэлт сонголт маягаар санал болгодог, хэрэглэгч гагцхүү “нууц” горимд шилжсэн тохиолдолд л үйлчилдэг байна.[97]

---

[92] L. Zhang, Facebook software engineer, Building Facebook Messenger, 12 August 2011, available at: www.facebook.com/notes/facebook-engineering/building-facebook-messenger/10150259350998920
[93] Facebook, Secure browsing by default, 21 July 2013.
[94] Stone Temple Consulting, Hard Numbers for Public Posting Activity on Google Plus, 14 April 2015, available at: www.stonetemple.com/real-numbers-for-the-activity-on-google-plus/ (accessed September 2016)
[95] Android Police, Google Duo has been downloaded 5 million times on Android since its release, 25 August 2016.
[96] Google, How Hangouts encrypts information, available at: https://support.google.com/hangouts/answer/6046115
[97] Google blog, Saying 🖐 to Allo and Duo, 18 May 2016, available at: https://googleblog.blogspot.co.uk/2016/05/allo-duo-apps-messagingvideo. html?_sm_au_=iVVS4PDKVHPkqLQ5

Хэнг-Аутс үйлчилгээнд төгсгөлийн шифрлэлт хийх нь техникийн талаасаа нилээдгүй төвөгтэй ба өмнөх хэрэглэгчдэд дахин танилцуулах шаардлага үүснэ. Ихэнх тохиолдолд байр сууриа олсон иймэрхүү үйлчилгээний хувьд хэрэглэгчид нь цахим хуудас болон бусад техникийн хэрэгслийг ашиглан программыг хэрэглээд дадчихсан байдаг.

Гэхдээ эдгээр асуудлууд нь тэгээсээ эхэлж буй шинэ Алло болон Дуо апликейшнд хамааралгүй ба зөвхөн гар утас, таблетанд ашиглана. Аллогийн бүх мессэж үйлчилгээнд төгсгөлийн шифрлэлт хийхгүй байх шийдвэр гаргасан шалтгаан нь бусад онцлог үйлдэлүүд – ялангуяа "Гүүгл Туслах"зэрэг нь ажиллах боломжгүй болно хэмээн Гүүгл мэдэгдсэн юм.[98] 2016 оны 5-р сард Аллог гаргах тухай зарлахад уг шийдвэрийг хувийн нууцлалтай байх эрхийг дэмжигчид хүчтэй шүүмжилсэн билээ. Апликейшнийг 2016 оны 9-сард гаргах үед өмнө нь Аллод оруулахаар амласан хувийн нууцлалыг бусад хамгаалалтыг оруулж өгөөгүй урчаас Гүүглийг дахин шүүмжлэлтэнд өртсөн юм.[99]

Гуравдагч талын заналхийлж буй хүний эрхийн эрсдлээс хангалттай урьдчилан сэргийлэхийн тулд Гүүгл бүхий л шуурхай шуудангийн үйлчилгээндээ төгсгөлийн шифрлэл нэвтрүүлэх ёстой. Ингэснээр хүний эрхийг хүндэтгэн хамгаалах үүргээ гүйцэтгэх боломжтой болно. Хиймэл оюун санааг төгсгөлийн шифрлэлтэй холбох нь техникийн хувьд маш хүндрэлтэй, төвөгтэй ажил гэдэг нь гарцаагүй.[100] Гэхдээ хэрвээ компани сул шифрлэлт бүхий нэмэлт үйлчилгээ/сонголттой өөр нэгэн горимыг үйлчилгээндээ оруулах бол үүнийгээ автомат ажилладаг байхаар тохируулж болохгүй. Сул хамгаалалт бүхий горимд шилжсэнээрээ хүний эрхэд нь ямар эрсдэл учирч болох тухай хэрэглэгчдэд тодорхой сануулга, дохио өгөх ёстой.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести Интернэшнлийн зүгээс 1 оноо өгөөд байна.

Дээр тайлбарласанчлан Гүүгл хувийн нууцыг хамгаалахаа олон нийтийн өмнө амлан, үүрэг хүлээсэн билээ. Ерөнхийдөө, хэрэглэгч Гүүглийн нийт үйлчилгээний хүрээнд бүгдэд нь нууцлал болон хувийн мэдээллийн тохиргоо хийх боломжтой гэдгийг харуулах олон материал, хэрэгсэл байна. Гэхдээ шуурхай зурвасын үйлчилгээний хэрэглэгчдэд тусгайлан зориулсан мэдээлэл тун ховор.

Компани өөрийн цахим хуудсандаа Мессенжэр үйлчилгээнд суурилуулсан шифрлэлтийн түвшний мэдээллийг байрлуулсан байна. Гэхдээ апликейшн дотор нь үйлчилгээнд ашиглагдаж буй шифрлэлт, хэрэглэгчдийн хүний эрхийн халдлагаас хэрхэн хамгаалж байгаа/хариу үзүүлж байгаа тухай хэрэглэгчдэд тодорхой мэдээлэл өгөх зүйл алга байна. Дуо болон Хэнг-аутс үйлчилгээний аль алинд шифрлэлтийн тухай дурьдсан зүйл огт байхгүй, зөвхөн компаний нууцлалын бодлогыг дарж үзэж болох холбоос байрлуулжээ. Аллогийн хувьд "нууц" горимд шилжих үед мессэжийг "дээд зэргийн нууцлалтай хадгална" гэх зурвас гарч ирдэг. Гэхдээ нууц ярианы явуулах үед хэрэглэгддэг шифрлэлтийн өөр өөр түвшний тухай тайлбар эсвэл автомат тохиргоог хэрэглэснээр тэдний харилцаа холбоо хэр сул хамгаалагдах тухай анхааруулга байдаггүй.

The Electronic Frontier Foundation (EFF) "Хэдийгээр Алло олон хэрэглэгчийг төгсгөлийн шифрлэлт бүхий мессэж ашиглах боломж олгодоггүй ч гэсэн хамгаалалттай мессэж үйлчилгээ ба энэ нь хэрхэн ажилладаг тухай Алло-н хоёрдмол сигналын учруулж болох хохирол нь уг үйлчилгээний цаашдын боломжийг хажууд л өчүүхэн юм гэжээ". [101]

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Эмнести Интернэшнл Гүүгл компанид уг шалгууруар 3 оноо өгчээ.

---

[98] E. Nakashima and H. Tsukayama, Los Angeles Times, Google chat app Alio boasts strong encryption - if you turn it on, 23 May 2016.
[99] Fortune, Everything You Need to Know About Google Allo's Privacy Backlash, 22 September 2016, available at: http://fortune.com/2016/09/22/google-allo-nope/
[100] Email correspondence with security engineer Frederic Jacobs, August 2016.
[101] EFF, Google's Alio Sends The Wrong Message About Encryption, 3 October 2016, available at: www.eff.org/deeplinks/2016/09/googles-allo-sends-wrong-message-a bout-encryption

Гүүглийн ил тод байдлын тайланд Засгийн газар хэрэглэгчийн мэдээлэл авахаар хүссэн хүсэлтийн тухай дэлгэрэнгүй мэдээлэл, зарим нэг мэдээлэл гаргаж өгсөн хүсэлтийн хувийг нийтэд нь болон улс улсаар нь тодорхой дэлгэсэн байна. Мөн компаний бодлогын дагуу ямарваа мэдээллийг дэлгэхээсээ өмнө холбогдох хэрэгчдэд зайлшгүй мэдэгддэг.[102]

2015 онд Гүүглийн ахлах ажилтнууд компани Засгийн газруудад үйлчилгээнд "арын хаалга" буюу нэвтрэх эрх олгодоггүй хэмээн мэдэгдсэн[103] боловч компани ба Гүйцэтгэх Захирал ч бусад технологийн компаниудтай адил "арын хаалга" нэвтрэх эрхийг эсэргүүцсэн байр суурыа олны өмнө батлаагүй билээ. Эмнести Интернэшнл Гүүглийн өөрийн мессэж үйлчилгээндээ "арын хаалга" суурилуулсан эсэхийг компаниас асуусан болон энэхүү номын хэвлэх хүртэл Гүүгл албан ёсоор хариулт өгөөгүй юм. Гэвч "арын хаалга" суурилуулсан гэх ямарваа нотлох баримт эсвэл олон нийтийн гомдол олдоогүй.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Эмнести Интернэшнл уг шалгуурийн хувьд Гүүгл-д 1 оноо өгсөн байна.

Allo (Алло) нь бүрэн нээлттэй эх сурвалжийн Сигнал шифрлэлтийн протокол хэрэглэдэг. 2015 оны 5-р сард Алло-г хэрэглээнд нэвтрүүлэх тухай зарлах үед Нээлттэй Шивнээ Систем буюу Сигналын эцэг компани "апликейшн хэрэглээнд нэвтрэх үед илүү дэлгэрэнгүй техникийн болон холболтын мэдээлэл өгөх болно" гэсэн байдаг".[104] Гэвч энэхүү номыг хэвлэх хүртэл энэ тухай хэвлэгдсэн мэдээлэл байхгүй байна. Дуо нь Гүүглийн зохион бүтээсэн QUIC гэх шинэ протокол хэрэглэдэг. Компани QUIC-ын крипто шифрлэлтийн техникийн мэдээллийг нийтлэсэн хэдий ч уг протокол нь Дуо-д хэрхэн ашиглагдаж буй тухай илтгэл тавиагүй.[105]

Гүүгл нь Хэнг-Аутс үйлчилгээндээ хэрэглэдэг тээвэрлэлт түүний шифрлэлтийн талаар тун товчхон тайлбар өгсөн байдаг.[106]

Гүүглийн зүгээс Алло-д нээлттэй эх сурвалж бүхий шифрлэлтийн протокол хэрэглэж байгаа нь таатай боловч компани бүх үйлчилгээндээ шифрлэлт хэрхэн хэрэглэж буй асуудал дээр илүү нээлттэй байх ёстой хэмээн дүгнэжээ.

KAKAO CORPORATION (КАКАО КОРПОРАЦИ)

Какао Корпораци нь Өмнөд Солонгосын технологийн компани юм. Уг корпорацийн олон үйлчилгээний дунд КакаоТоК гэх мессэжийн апликейшн байдаг. Уг апликейшныг сар бүр 49 сая илүү хэрэглэгч идэвхитэй ашигладаг байна.[107] КакаоТоК-ыг Өмнөд Солонгост өргөн хэрэглэдэг ба 2014 онд Какао-ийн Гүйцэтгэх Захирал Өмнөд Солонгос улсын ухаалаг гар утас эзэмшигчдийн 93% нь КакаоТоК-ыг хэрэглэдэг хэмээн мэдэгджээ.[108]

2014 оны 10-р сард Севол усан онгоцын гамшгийн хэргийг Засгийн газар хэрхэн шийдвэрлэж байгааг шүүмжилсэн хэрэглэгчдийн мэдээллийг дэлгэ гэх Солонгосын Засгийн газрын шаардлагыг тусгасаны улмаас Какао нь олон нийтийн зүгээс асар их шүүмжлэлд орсон байна.[109] Үүний хариуд Компаний Гүйцэтгэх Захирал "манай хэрэглэгчдийн хувийн яриаг хянах гэсэн аливаа шүүн байцаах тушаал"-ыг хүлээн авахгүй гэдгээ мэдэгджээ.[110] Улмаар компани шифрлэлтийн түвшинээ дээшлүүлэх, ил тод байдлаа сайжруулах чиглэлээр томоохон алхам авч хэрэгжүүлсэн байдаг.

[102] Google Transparency Report, available at: www.google.com/transparencyreport/userdatarequests/legalprocess
[103] Speech by Rachel Whetstone, Google's Senior Vice President Communications and Public Policy, 13 February 2015, available at: http://googlepolicyeurope.blogspot.co.uk/2015/02/privacy-security-surveillance-getting.html
Statement by Rob Salgado, Google's Director for law enforcement and information security, 8 May 2015, available at: www.reddit.eom/r/IAmA/comments/35b6bt/we_are_senior_members_af_googles_public_policy/cr2sd65
[104] Open Whisper Systems, Open Whisper Systems partners with Google on end-to-end encryption for Alio, 18 May 2016.
[105] Google, QUIC Crypto Specification, 26 May 2016, available at: https://docs.google.com/document/d/lg5nlXAIkN_Y- 7XJW5K45lblHd_L2f5LTaDUDwvZ5L6g/edit
[106] Google, How Hangouts encrypts information.
[107] Statista, Number of monthly active KakaoTalk users from 1st quarter 2013 to 2nd quarter 2016, available at: www.statista.com/statistics/278846/kakaotalk-monthly-active-users-mau/
[108] Keynote speech by Lee Sir-goo, CEO of KakaoTalk, at the Mobile World Congress, 24 February 2014, available at: www.koreaherald.com/view.php?ud=20140224001578 (accessed September 2016)
[109] Y. Lee, Associated Press, S. Korea rumor crackdown jolts social media users, 5 October 2014.
[110] Korea Times, Kakao defies prosecution's monitoring, 14 October 2014, available at: www.koreatimesus.com/kakao-defies-prosecutions-monitoring/

Какао Эмнести Интернэшнлийн мэдээлэл авах гэсэн хүсэлтэнд зохих хариуг өгсөн юм.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Уг шалгуурт Эмнести Интернэшнл Какао-д 1 оноо өгөв.

Какао өөрийн нууцлалын бодлогодоо заасан амлалтаа сахин биелүүлэхээ мэдэгдсэн юм. Компаний цахим хуудсандаа шифрлэлт гэх хувийн нууцлалыг хамгаалах чиглэлээр авч буй арга хэмжээний тухай дурьдсан байна.[111] Эмнести Интернэшнлийн захидалд хариулахдаа Какао хэрэглэгчдийнхээ үзэл бодлоо чөлөөтэй илэрхийлэх эрх чөлөөг хамгаалахаа амлажээ. 2016 оны 5-р сард ТББ ЯГ ОДОО-д бичсэн захидалдаа компани хэрэглэгчдийнхээ үзэл бодлоо чөлөөтэй илэрхийлэх эрх чөлөө, хувийн нууцлалыг хамгаалах амлалтынхаа нэгэн адил удахгүй соёрхон батална гэжээ. Бид уг ажлаа 2016 оны 3-р улирал гэхэд дуусгахаар ажиллаж байна.[112]

Эмнести Интернэшнл-д бичсэн хариундаа компани хувийн нууцтай байх эрх, үзэл бодлоо чөлөөтэй илэрхийлэх эрхийг хамгаалахын тулд авч хэрэгжүүлэх зарим арга хэмжээний тухай цохон тэмдэглэжээ.

Олон төрлийн мэдээлэл ба өмнөх туршлага зэрэг дээрээ суурилан Какао нь мессэжийн үйлчилгээн дэх хяналтын цонх мөн эрсдлийн менежментийн загвар зэргийг болгоомжтойгоор дахин нягталж үзсэн байна.[113] Тус компани хакеруудаас ирэх болзошгүй аюул занал эсвэл санаа зовоосон ямар нэгэн шинжтэй асуудал зэргийг онцлон авч үздэг аюулгүй байдлыг хангах үйл ажиллагааны төвтэй байна.

Гэвч компани Засгийн газрын хууль бус хяналт болон цахим гэмт хэрэг нь мессэж үйлчилгээ хэрэглэгчийн эрхэд хэрхэн заналхийлж буйг Гүүгл хүлээн зөвшөөрөөгүй байна. Какао уг үнэлгээг эсэргүүцэн өөрийн цахим хуудсын аюулгүй байдлын хэсэг дэх мэдэгдэлд "манай байгууллага Какао нь гадны гуравдагч этгээдээс хэрэглэгчдийнхээ мэдээллийг хамгаалах үүргээ хэзээ ч орхигдуулахгүй" гэжээ.[114] Хэдийгээр уг мэдэгдэл нь компаний хэрэглэгчдийн хувийн нууцыг хамгаалах үүрэг амлалтыг илэрхийлж байгаа боловч хүний эрхэнд цахимаар халдаж буй эх сурвалжийг хангалттай таньж, хүлээн зөвшөөрсөн гэж үзэхгүй байна.

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Уг шалгууураар Какао-д 1 оноо өгсөн байна.

Какао нь КакаоТоК-д төгсгөлийн шифрлэлт ашигаладаг боловч үүнийг автоматаар ажилладаг байхаар тохируулаагүй байна. Төгсгөлийн шифрлэлт ашиглахын тулд хэрэглэгчид "нууц яриа" нэмэлт сонголтыг сонгох ёстой. КакаоТоК-аар дамжиж буй бусад мессэж нь тээвэрлэлт түүний түвшний шифрлэлттэй байдаг өөрөөр хэлбэл шифрийг тайлсан мессэжийг Какао-н сервэрээс авах боломжтой ажээ.

Какао Эмнести Интернэшнлийн асуулгад хариулахдаа "Нууц яриа" нь бусад 2 автомат горим (нээлттэй яриа болон энгийн яриа)-той нэгэн адил автомат горим мөн гэв. Яриа цонх дээр даран шинэ яриа эхлүүлэх бүрт эдгээр 3 сонголт нь зэрэгцэн гарч ирдэг боловч найзууд цонхоор дамжуулан яриа хийхэд автоматаар "энгийн яриа" горимыг сонгодог байна. Энэ "энгийн яриа" нь автомат горим болохыг харуулж байна.

КакаоТок-аар явж буй нийт мессэжинд төгсгөлийн шифрлэлт хийхгүй байх шийдвэрээ компани өнөөг хүртэл бүрэн тайлбарлаагүй байна. Яг Одоо-д явуулсан захидалдаа компани

[111] Kakao, Privacy Policy: Technical Measures, available at: http://privacy.kakaocorp.com/en/protection/tech
[112] Kakao letter to Access Now, 2 May 2016, available at: httpsV/business- humanrights.org/sites/default/files/documents/Kakao%20response.pdf
[113] Kakao letter to Amnesty International, 12 July 2016.
[114] Kakao letter to Amnesty International, 4 October 2016.

"КакаоТоК-ын бүх ярианд төгсгөлийн шифрлэлт хийхэд бидэнд зарим нэг функцын болоод техникийн хүндрэлүүд тулгараад байгаа боловч бид төгсгөлийн шифрлэлт хэрэглэх асуудлыг нухацтай бодолцон үзэж байгаа" гэжээ.[115]

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести Интернэшнл уг шалгууруар шүүн 1 оноо өгөөд байна.

Какао нь цахим хуудасныхаа нууцлал, хувийн мэдээллийг хэрхэн цуглуулж, хэрэглэдэг болон "Нууц яриа" горимын тухай хэрэглэгчдэд ойлгомжтой байдлаар бэлтгэн байршуулжээ.

Гэхдээ компани КакаоТоК-ыг хэрэглэх үед хэрэглэгчдийн эрхэд ямар эрсдэл учирч болохыг сануулдаггүй ба ингэхдээ автомат ярианы горим ашиглах үед хувийн захидал харилцаа нь задрах илүү эрсдэлтэй байдаг тухай мэдэгддэггүй.

Апликейшнийг хэрэглэн шинэ яриа эхлүүлэх үед "Нууц яриа" горимыг сонгох сонголт ил байдаг. Гэвч программын дотор шифрлэлт гэж юу болох, нууц болон энгийн ярианы ялгааны тухай тайлбар байхгүй. Илүү сул түвшний шифрлэлт хэрэглэснээр хэрэглэгчийн эрхэд учирч болох эрсдэлийг мөн сануулсан зүйл байхгүй.

Эмнести Интернэшнлд өгсөн хариундаа Какао "апликейшн дотор тайлбар өгөхөөсөө илүү цахим хуудас, албан ёсны блог, хэвлэл мэдээлэл болон бусад олон төрлийн цахим материалаар дамжуулан нууц ярианы горимыг тайлбарлан таниулахаар шийдсэн. Ингэснээр КакаоТоК үйлчилгээг алдаагүй явуулах боломжтой болно."

Компани хэрэглэгчиддээ эрхийг нь шифрлэлтээр дамжуулан хэрхэн хамгаалж байгаа, өөр өөр түвшний хамгаалалтын ямар горимууд байгаа зэрэг мэдээллийг апликейшн дотор нь оруулж өгөх нь чухал хэмээн Эмнести Интернэшнл үзэж байна.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Уг шалгуурын тухайд Эмнести Интернэшнл Какао-д 3 оноо өглөө.

2015 оны 1-р сараас эхлэн Какао нь ил тод байдлын тайлан гарган 2013 оноос хойш Өмнөд Солонгосын Засгийн газрын мэдээлэл авах хүсэлтийн тоо, хүсэлтийн агуулга болон үүнд өртсөн хэрэглэгчдийн хаягийн тоо зэргийг дэлгэжээ. Какао нь ил тод байдлын тайлан гаргасан анхны Өмнөд Солонгосын компани болсон билээ.

Өмнөд Солонгос улсын хуулиар тухай этгээдийн яллах эсвэл баривчлах шийдвэр гаргаснаас хойш 30 хоногийн дотор хэрэглэгчдэд харилцаа холбооны хяналт тавих болсон тухай мэдэгдэх ёстой ажээ.[116] Харилцаа холбооны агуулгын тухайд мэдээлэл дэлгэсэн компани нь хэрэглэгчдээ мэдэгдэх боломжгүй байдаг байна.[117] Уг асуудлын тухайд Какао Эмнести Интернэшнлд хэлэхдээ "бид хэрэглэгчдийн эрх, тэдний мэдэгдэл авах боломжийг нэмэгдүүлэхийн тулд ярилцаж, өнөөгийн хуулийн хүрээнд хамгийн боломжит хууль ёсны шийдлийг олох гэж оролдсон. Цаашилбал, хэрэглэгчдэд харилцаа холбоог нь хянаж байгаа тухай мэдэгдэх асуудлыг хууль тогтоогчид шийдвэрлэх болно" гэжээ.[118]

Гэвч Какао хэрэглэгчдийн хувийн мэдээллийг авах хүсэлт ирсэн үеэс эхлээд хэрэглэгчдэд мэдэгддэг эсэх нь тодорхойгүй байна. Өмнөд Солонгос улсын хуулиар прокурор эсвэл цагдаа нь тухайн хэрэглэгчдийн мэдээлэл авах талаараа бичгэн хүсэлт хүсэлт илгээх ёстой бөгөөд Какаогийн зүгээс хэрэглэгчдэд мэдэгдэх явдлыг сайжруулах аливаа яриа хэлэлцүүлэгт идэвхитэй оролцоно хэмээн мэдэгдсэн юм.[119]

---

[115] Kakao letter to Access Now, July 2016
116 Korea Internet Transparency Report, section on Surveillance, available at: http://transparency.kr/surveillance?ckattempt=l
[117] K.S. Park, Professor, Korea University Law School, Communications Surveillance in Korea, August 2014, section 4, available at: http://opennetkorea.org/en/wp/main-privacy/internet-surveillance-korea-2014?ckattempt=2#_ednrefl
[118] Kakao letter to Amnesty International, 4 October 2016.
[119] Kakao Privacy Policy, Frequently Asked Questions, available at: http://privacy.kakaocorp.com/en/faq/report/pagel .

Мөн Эмнести Интернэшнл-д бичсэн захидалдаа Какао өөрийн мессэж үйлчилгээндээ "арын хаалга"-аар нэвтрэх тохиргоо хийдэггүй, мөн Засгийн газраас арын хаалгаар нэвтрэх тохиргооны ямарваа хүсэлт хүлээн аваагүй хэмээн мэдэгдсэн."

Цаашилбал Какао нь харилцаа холбооны мэдээлэл эсвэл төгсгөл хоорондын шифрлэлтийг хэрэгжүүлэхэд саад болох гэсэн төрийн эрх баригчдын аливаа шаардлагыг хүлээн авдаггүй" хэмээн мэдэгдэв. Эмнести Интернэшл компани 2014 онд олон нийтийн шахалтаар нууцлалын хамгаалалтаа чангатгаснаас хойш уг байр сууринаасаа ухарсан гэх ямарваа сэжиг эсвэл нотлох баримт олоогүй юм.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Энэ шалгууураар Эмнести Интернэшнл Какао-д 0 оноо өгөөд байна.

Эмнести Интернэшнлийн асуултын хариуд Какао өөрийн цахим хуудсан дээрээ КакаоТоК-аар явагдаж буй харилцаа холбоог хэрхэн шифрлэдэг тухайгаа товч тайлбарлан байрлуулсан юм. Эмнести Интернэшнл компани шифрлэлт хэрхэн хийдэг тухай өөр дэлгэрэнгүй мэдээлэл олж чадаагүй. Какао өөрийн LOCO харилцаа холбооны протоколыг ашигладаг.

Line (Лайн)

Япон улсын Лайн корпорацийн үндсэн бизнес нь гар утасны зурвас илгээх үйлчилгээ юм. Энэ компани нь Өмнөд Солонгосын интернэт үйлчилгээний Навер корпорацийн Япон дахь охин компани билээ. Лайн компаний апликейшн нь өдөрт 200 сая гаруй идэвхитэй хандалт авдгаараа Япондоо түүнчлэн Индонез, Тайлан болон Тайваны зах зээлийн гол компани юм.[120]

Лайн нь Эмнести Интернэшнлийн мэдээлэл авах хүсэлтэнд хариулсан болно.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Уг шалгуурт Лайн компанид 1 оноо өгөөд байна.

Компаний нууц хадгалах журмын дагуу хэрэглэгчдийнхээ хувийн мэдээллийг хамгаалах үүрэгтэй байдаг. Япон Улсын хуулийн дагуу үзэл бодлоо чөлөөтэй илэрхийлэх эрхийг хамгаалах асуудлыг компаний вебсайт дээр заасан байна.

Мөн хэрэглэгчийн мэдээллийг хамгаалдаг арга хэмжээгээ нарийвчлан заасан байдаг ба үүнд нь шифрлэлт ашиглах тухай заасан байна.[121] Компани нь "өндөр нууцлал бүхий шифрлэлт, гуравдагч этгээд нэвтрэхээр оролдоход хариу арга хэмжээ авах"-аар апликейшнээ шинэчлэх болон түүний мэдээллийг задлахаасаа өмнө хамгаалалтын шалгалтууд хийдэг байна.[122]

Гэсэн хэдий ч Лайн компани, ямар нэгэн хяналтаас үүсэх аюулаас хүний эрхийг хэрхэн хамгаалах эсвэл шифрлэлтийг хамгаалах үед авах арга хэмжээний талаар дурдаагүй байна.

"Лайн Корпораци нь Төрийн хяналт шалгалттай холбоотойгоор мэдээлэл задлах тухай аливаа хүссэлтийг хүлээн авч, хамтран ажилладаггүй болно" гэсэн аливаа халдлагаас хамгаалах мэдэгдэл хийгээгүй байна.

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл үүнд ердөө 3 оноо өгсөн юм.

---

[120] The Financial Times, *Line app looks to export Asian popularity to new markets*, 4 June 2016.
[121] LINE, LINE CORPORATION'S COMPLIANCE WITH APPLICABLE LAWS, section on Telecommunications Business Act-Communications secrecy., available at http://linecorp.com/en/security/article/34
[122] LINE, secure programming available at http://linecorp.com/en/security/article/38

2016 оны 6-р сард, Лайн компани эх бичвэр, мессэж, VoLP, дүрст дуудлага зэргийг нэвтрүүлэхийн тулд төгсгөл хоорондын шифрлэлтийг илүү өргөжүүлжээ.[123]

Урьд өмнө нь төгсгөл хоорондын шифрлэлт нь зөвхөн сонголт маягаар харагдах боломжтой байжээ.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести Интернэшнлийн зүгээс 1 оноо өгөөд байна.

Лайн компани нь “бид салбарынхаа өндөр туршлага дээр тулгуурлан хувийн мэдээллийн нууцлал болон хамгаалалтын аргаа тогтмол шинэчилдэг” хэмээн Эмнести Интернэшнлд мэдэгдсэн.

Лайн компаний вебсайт дээр хэрэглэгч хувийн мэдээллээ хэрхэн хамгаалах аргачлалыг мөн апликейшнээрээ шифрлэлтийн түвшингөө тогтоох бололцоогоор хангасан байдаг. Үүгээрээ хүмүүсийн мэдээлэл нь “зөвхөн гуравдагч этгээд төдийгүй сервэр ажилтануудаас нуугддаг” болохыг харуулж байна. Гэсэн ч компани хэрэглэгчиддээ Засгийн газрын хууль бус хяналт болон цахим гэмт хэргээс сэргийлсэн анхааруулга хийгээгүй.[124] Мөн мессэжний апликейшн нь ямар түвшний шифрлэлтийн тохиргоотой болох талаар хэрэглэгчид зориулсан мэдээлэл, мэдэгдэл байхгүй, хэрэглэгчийн эрхийн эсрэг ямар нэгэн эрсдэл гарахад түүнээс урьдчилсан сэргийлэхээр шифрлэлтийг хэрхэн автоматжуулсан тухай мэдээлэлгүй байна.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Эмнести Интернэшл тус шалгуурын тухайд Лайн компанид 1 оноо өгсөн юм.

Лайн Засгийн газраас мэдээлэл авах тухай хэдэн хүсэлт ирсэн, түүний агуулгын тухай мэдээллийг нийтэд ил тодоор мэдээлдэггүй. Тэдний вебсайт дээр “санаачлагуудыг хэрэгжүүлэх энэхүү хэрэглэгчийн мэдээллийг хамгаалах арга хэмжээ авахаар төлөвлөгөж байна” хэмээн мэдээлсэн байна.

Лайн нь Засгийн газрын хүсэлтийг хэрхэн шийдвэрлэх тухай багахан дурдсан: “Лайн компани төрийн эрх бүхий байгууллагаас баталсан шийдвэр, тушаалын үндсэн дээр нууц мэдээллийг хамгаалах журмын дагуу зөвхөн гэмт хэргийн мөрдөн шалгах ажиллагаанд хамтран ажиллана” гэжээ. Гэвч энэ нь хувь хүний мэдээллийг авах хүсэлт гаргахад түүнд мэдэгдэнэ гэсэн үг биш юм.

Мөн шифрлэлтийн үйлчилгээндээ арын хаалгаар нэвтрэх тохиргоо хийдэггүй гэдгээ онцолсон байна. Энэ талаар Эмнести Интернэшнлд өгсөн тайлбартаа одоогийн үйлчилгээнд ямар ч арын хаалга байхгүй ба энэ тухай ямар ч хүсэлт хүлээн аваагүй “мөн бид Засгийн газраас арын хаалгаар мэдээлэл авах хүсэлт ирвэл түүнийг хүлээн авахгүй” хэмээжээ.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Эмнести Интернэшнл энэ шалгуурт Лайнд 1 оноо өгчээ.

Лайн апликейшндээ ашигладаг шифрлэлтийн системийн талаарх ерөнхий мэдээллийг вебсайт дээрээ нийтэлсэн байна.[125] 2016 оны 09-р сард тус компани аюулгүй байдлын инженерүүд болон алгоритмын ашиглалт, шифрлэлтийн протоколын техникийн нарийн мэдлэгтэй хөгжүүлэгчдэд техникийн (whitepaper) засгийн газрын илтгэлийг нийтэлжээ.[126]

[123] LINE,Hidden Chat users to enjoy “Letter Sealing” from July,30 june 2016
[124] LINE, *Data Security*, available at: https://linecorp.com/en/security/article/37
[125] Spiegel, *Inside the NSA’s War on Internet Security*, 28 December 2014, available at: www.spiegel.de/international/germany/inside-thensa-s-war-on-internet-security-a-1010361.html
[126] LINE, *Encryption Overview: Technical Whitepaper*, 29 September 2016, available at: https://scdn.line-apps.com/stf/linecorp/en/csr/lineencryption-whitepaper-ver1.0.pdf

Гэвч өөрсдийн шифрлэлтийн протоколоо ашиглаж байгаа ба энэ нь хаалттай эх сурвалжид тооцогдох юм.

MICROSOFT (Майкрософт)

Скайп нь суурин софтвэйр болон гар утсанд хэрэглэгддэг харилцаа холбооны хэрэгсэл ба олон улсын хэмжээний компани болох Майкрософт компаний 2011 үүсгэн байгуулагдсан салбар нэгж юм. Скайп нь 300 сая орчим хэрэглэгчтэй бөгөөд дуут, дүрст болон бичгэн зурвас илгээдэг.[127] Засгийн газрын хууль бус хяналт шалгалтын гол бай нь байсаар ирсэн, Засгийн газар Скайпын мэдээлэлд нэвтрэх эрхтэй байдаг нь нэгэнт ил болсон.[128]

Эдуард Сноудений нийтэд дэлгэсэн мэдээлэл нь Үндэсний Тагнуулын Албаны дуут, дүрст болон бичгэн зурвасыг татаж авах үйлдэлтэй PRISM (ПРИЗМ) программын тусламжтайгаар боловсруулсан "Скайпын мэдээллийн цуглуулга" байсан юм.

Майкрософт худалдаж авахаас өмнө, Скайп нь АНУ-ын Тагнуулын алба болон хууль сахиулах хүчний байгууллагуудын дотоод хэрэгцээндээ хоорондоо дуудлага хийх зорилгоор бүтээгдсэн нууц программ байсан гэж 2013 онд Нью Йорк Таймс мэдээлсэн.

Өмнөх хугацаанд Скайпын Хятад түнш болон TOM-Скайп компанийг чиглэсэн Хятадын Засгийн газраас хууль бус хяналт, шахалт ирсэн байдаг.[129] Улмаар 2013 онд Майкрософт нь хэрэглэгчдийнхээ хувийн мэдээллийн нууцлалыг чангатгахын тулд TOM групптэй хийсэн харилцаагаа дуусгавар болгосон байна.[130]

Төрийн хууль бус хяналт шалгалтын асуудлууд Скайпын түүхэнд байдаг ба одоо ч шифрлэлтийг ашиглахдаа сул байгаа.[131] Гэхдээ Майкрософт бол хүний эрхийн өмнө хүлээсэн өндөр хариуцлагатай компани бөгөөд хүний эрхийг дээдлэх бодлого журмыг харьцангуй ил тод болгодог. Компани нь Скайпынхаа шифрлэлтийн бодлогоо чангатгах үүргийг заавал дагаж мөрдөх үүрэгтэй ба түүнчлэн хүний эрхийг хамгаалахын тулд шифрлэлтийг хэрхэн ашигладаг талаар өөрийн хэрэглэгчдэд илүү нээлттэй мэдээллэх ёстой.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Уг шалгуурт Майкрософт компанид 3 оноо өгөөд байна.

Майкрософт Олон улсын хүний эрхийн хэм хэмжээний зөвлөмжинд заасан хүний эрхийн тунхаглалдаа хүний эрхийг дээдлэх, үзэл бодлоо чөлөөтэй илэрхийлэх эрхийн талаар нийтийн өмнө хүлээсэн үүргээ маш тодорхой болгосон.

Мөн "бид таны итгэж өгсөн мэдээллийн нууцлалыг хадгалах аюулгүй байдлын хүчирхэг тогтолцоотой ба тэр дундаа шифрлэлтийг ашигладаг" гэсэн асуулга бүхий хувийн нууцыг хэрхэн хадгалах талаар зургаан үндсэн хувийн нууцлалын зарчимтай.[132] Глобал сүлжээний асуудал, Засгийн газрын ажиглалттай хамтын ажиллагаагаар дамжуулан хувийн нууцтай байх эрх болон үзэл бодлоо чөлөөтэй илэрхийлэх эрхийн эсрэг цахим аюул заналыг илрүүлдэг.[133]

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл үүнд ердөө 0 оноо өгсөн юм.

---

[127] Statista, *Leading social networks worldwide as of September 2016, ranked by number of active users*, September 2016.
[128] Spiegel, *Inside the NSA's War on Internet Security*, 28 December 2014, available at: www.spiegel.de/international/germany/inside-thensa-s-war-on-internet-security-a-1010361.html
[129] The New York Times, *Web's Reach Binds N.S.A. and Silicon Valley Leaders*, 19 June 2013, available at: www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html?_r=1
[130] See for example: N. Villeneuve, P. Fellow, the Citizen Lab, Breaching Trust: An analysis of surveillance and security practices on China's TOM-Skype platform, 1 October 2008; Reuters, Skype says China JV partner stores text messages, 2 October 2008; TechCrunch, Skype Must Be More Transparent, Says Activists And Advocacy Groups, 24 January 2013.
[131] Reuters, *Microsoft blocks censorship of Skype in China: advocacy group*, 27 November 2013.
[132] Microsoft, *Global Human Rights Statement*, available at: www.microsoft.com/about/csr/DownloadHandler.ashx?Id=03-01-01
[133] Statement by Microsoft CEO Satya Nadella, *Privacy at Microsoft*, available at: https://privacy.microsoft.com/en-US/

Компани Эмнести Интернэшнлд илгээсэн захидалдаа, Скайп нь энэ төрлийн үйлчилгээ үзүүлдэг апликейшнуудад нийтлэг хэрэглэдэг стандарт шифрлэлтийг ашигладаг бөгөөд Спайпаар явуулж буй бүх дуудлагад төгсгөлийн шифрлэлт хэрэглэдэг гэжээ.

Гэхдээ компаний зүгээс шифрлэлтийн түлхүүр хэрхэн боловсруулдаг ангилал, Скайп дуудлага хийхэд хэрхэн ширфлэлт ажилладаг —ялангуяа Скайп ширфлэлтийн түлхүүрийг дотооддоо хадгалдаг эсэх- тухай мэдээллээ өгөөгүй болно.[134] Мөн энгийн дугаар руу залгах боломж олгодог аливаа апликейшний нэгэн адилаар интернэтийн орчин биш харин энгийн сүлжээ рүү орж байгаа хэсэг нь шифрлэлтгүй байдаг хэмээн мэдэгджээ.

Шуурхай зурвасын тухайд Майкрософт өөрийн цахим хуудсандаа төгсгөлийн шифрлэлт хэрэглэдэггүй тухайгаа тодорхой тайлбарласан ба хэрэглэгч болон Скайп-ын сервэрүүдийн хооронд шифрлэлт хэрэглэдэг гэжээ.[135]

Цааш нь Майкрософт болон Скайп төгсгөлийн шифрлэлт хийх нь орчуулгын хэрэгсэл зэрэг бүтээгдэхүүний зарим функц-д нөлөөлдөг тул тохируулага хийхэд хүндрэлтэй байдаг тухай мэдэгдсэн юм.

Бидэнд олдсон мэдээллээс үзэхэд Майкрософт компаний харилцаа холбооны агуулгад нэвтрэхээс хамгаалах ямарваа нэгэн хамгаалалтыг Скайпд хийж, төгсгөлийн шифрлэлт огт хийдэггүй байна. Иймд Майкрософт үйлчилгээндээ хангалттай шифрлэлт хийдэггүй хэмээн Эмнести үзэж байна.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести үүнд мөн л 0 оноо өгөөд байна.

Майкрософтийн цахим хуудсан дахь Нууцлалын Мэдэгдэлдээ хэрхэн хувийн мэдээллийг цуглуулж, хэрэглэдэг болон хуваалцдаг тухай мэдээллийг байрлуулжээ. Үүнд "бид танай материал, захидал харилцааг цуглуулан танд хэрэгцээтэй бүтээгдэхүүнийг санал болгохдоо хэрэглэдэг... цуглуулж авсан мэдээллээс нэр дурьдвал Скайп зэрэг Майкрософтоор илгээсэн болон хүлээн авсан захидал харилцаа" гэжээ.[136]

Эмнестид өгсөн хариу захидалдаа "хэрэглэгчиддээ зориулсан цахим тусламж үзүүлэх сувагтай бөгөөд үүнд Байнга Асуудаг Асуултууд хэсэгт Скайпын санал болгож буй бүхнийг тусгасан" бөгөөд Скайпд хэрэглэдэг шифрлэлтийг тайлбарласан холбоосыг мөн оруулсан байна. Гэхдээ дээр тайлбарласан шигээр Скайпын ярианд чухамдаа ямар шифрлэлт хэрэглэдэг, түлхүүрийг хэрхэн боловсруулдаг болон хуваалцдаг болон компани нь хэрэглэгчийн захидал харилцаанд нэвтэрдэг эсэх тухай мэдээллийг тодорхой заагаагүй байна.

Скайп апликейшны хувьд хэрэглэгчдэд шифрлэлтийн тухай ямарваа мэдээлэл өгдөггүй. Дуудлага хийх эсвэл зурвас явуулах зэрэгт аль түвшний шифрлэлттэй тухай хэрэглэгчдэд ойлголт байдаггүй ажээ. Скайпын шифрлэлтийн түвшин маш сул мөн хяналт хийн Скайпын харилцаа холбоонд хандсан тохиолдлууд гарч байсан учраас энэ нь ихээхэн асуудал үүсгэж байна.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Үүнд Эмнести 3 оноо өгөөд байна.

Майкрософт өөрийн цахим хуудасны ил тод байдлын хэсэгт хагас жил тутам ил тод байдлын илтгэлээ гаргадаг бөгөөд үүндээ дэлхий даяар хууль сахиулах байгууллагуудын хүсэлт болон АНУ-ын Засгийн газраас ирүүлсэн хууль ёсны шаардлагыг дэлгэдэг. Тус тайланд Скайп зэрэг Майкрософт компаний гаргасан бүх бүтээгдэхүүн, үйлчилгээг оруулсан байна.

[134] Microsoft, *Does Skype use encryption?*, available at: https://support.skype.com/en/faq/FA31/does-skype-use-encryption
[135] Microsoft, *Does Skype use encryption?*
[136] Microsoft Privacy Statement, August 2016, available at: https://privacy.microsoft.com/en-us/privacystatement/

Эмнестид илгээсэн тайлбартаа "Хэрвээ Засгийн газар хэрэглэгчийн мэдээллийг авахыг хүсвэл холбогдох хууль журмын дагуу хүсэлтээ гаргах ёстой. Өөрөөр хэлбэл хэрэглэгчийн мэдээлэл рүү нэвтрэх шүүхийн шийдвэр, захирамжийг бидэнд гаргаж өгөх ёстой. Бид мөн аль нэг цахим хаяг эсвэл хүн рүү хандан хүсэлтийг хүлээн авдаг" гэжээ.

Компани нь хуулиар хориглоогүй эсвэл онцгой нөхцөл байдал биш бол "хууль сахиулах болон Засгийн газрын бусад байгууллагаас мэдээллийг нь авахыг хүссэн хэрэглэгчдэд компани урьдчилан мэдэгдэх" бодлоготой. Майкрософт хэрэглэгчдийн мэдээллийг авах гэсэн Засгийн газрын хүсэлтийн нээлттэй байдлыг нэмэгдүүлэх алхмууд авчээ. АНУ-ын Засгийн газрын эсрэг хувийн нууцтай байх эрх ба ил тод байдалтай холбогдуулан дөрвөн нэхэмжлэл гаргасан байна. Хамгийн сүүлийн нэхэмжлэлийг 2016 оны 4-р сард гаргасан ба мэдээллийг хууль ёсоор шаардахдаа хэрэглэдэг нууцлалыг хадгалах тушаал Засгийн газар гаргадгийг шүүмжилжээ.[137]

Түүнчлэн "Майкрософт нь зурвас явуулах үйлчилгээнийхээ шифрлэлтэд "арын хаалга"-ны нэвтрэх эрх олгодоггүй...

Аль ч улсын Засгийн газарт хэрэглэгчдийн мэдээлэлд шууд, хязгаарлалтгүйгээр нэвтрэх эрх байдаггүй ба шифрлэлтийн түлхүүр болон шифрлэлтийг задлах чадварыг хэнд ч олгодоггүй" ажээ. Дээр тайлбарласан шигээр өмнө нь Скайп хэрэглэгчдийнхээ холбоо харилцаанд дур мэдэн нэвтрэх эрх олгож байна гэх сэжиг байсан боловч Майкрософт зөвхөн "нэр бүхий тодорхой цахим хаяг эсвэл хүн"-ий мэдээллийг авах гэсэн хууль ёсны шаардлагыг л биелүүлдэг хэмээн дахин дахин мэдэгдсэн юм.

Уг шалгууруар ерөнхийдөө Майкрософт Засгийн газрын хүсэлтийг хүлээн авсан тухайгаа ил тод байлгах зорилт тавин ажилладаг гэж дүгнэв. Гэхдээ хэрэглэгчдэд тэдний хүний эрх хамгаалагдаж байгаа гэдгийг бодитоор батлах зүйл бол хүчтэй шифрлэлт хэрэглэх явдал юм.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Уг шалгууруар Эмнести Майкрософтод 0 оноо өгчээ.

Майкрософт Скайп-даа хэрэглэдэг ширфлэлтийнхээ алгоритмын үндсэн мэдээллийг л олон нийтэд дэлгэсэн байна.[138] Скайп дуудлагад ямар шифрлэлт хийгддэг нь тодорхой бус бөгөөд шифрлэлтээ үйлчилгээнд хэрхэн хэрэгжүүлдэг нь тодорхой бус байна.

SNAPCHAT (Снапчат)

Snapchat (Снапчат) нь АНУ-д төвтэй компани, түүний гол бүтээгдэхүүн нь Снапчат гар утасны программ юм. Энэ нь хэрэглэгчид бие биедээ зураг болон дүрст мессэж буюу "Снайп" явуулах боломж олгоод зогсохгүй текст мессэж (Чат) бичих боломж олгодог. Бусад шуурхай зурвасын үйлчилгээнүүдээс ялгаатай нь эдгээр мессэжүүдийг нээсний дараа мессэж нь апликейшны холболтоос арилдаг. Өдөр бүр 100 сая илүү хүн хэрэглэдэг бөгөөд уг апликейшн нь залуучуудын дунд түгээмэл ашиглагддаг.[139]

Снапчат нь мэдээлэл авах гэсэн Эмнести Интернэшнлийн хүсэлтэд хариу өгсөн юм.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Эмнести Интернэшнл уг шалгууруар Снапчат-д 1 оноо өгсөн байна.

[137] B. Smith, Microsoft's President and Chief Legal Officer, *Keeping secrecy the exception, not the rule: An issue for both consumers and businesses*, 14 April 2016, available at: http://blogs.microsoft.com/on-the-issues/2016/04/14/keeping-secrecy-exception-not-rule-issueconsumers- businesses/#EwUCXsXzTmxiu6qG.99

[138] Microsoft, Does Skype use encryption?

[139] Snapchat letter to Amnesty International, 11 July 2016 (Snapchat letter); Statista, *Distribution of Snapchat users worldwide as of 2nd quarter 2015, by age,* 2016, available at: www.statista.com/statistics/315398/snapchat-user-age-distribution/

Эмнести Интернэшнлд илгээсэн захидалаа компани нь “хувийн нууцлал, аюулгүй байдал бол Снапчатын хамгийн суурь үнэт зүйл” юм гэжээ.[140] Уг зарчим нь компаний Нууцлалын Бодлогод тусгалаа олсон байна. Гэвч Снапчат компанид үзэл бодлоо чөлөөтэй илэрхийлэх эрх чөлөө зэрэг хүний бүхий л эрхийг хүндэтгэн хамгаалах тухай тусгасан бодлого байдаггүй.

“Бид манай системийн аюулгүй ажиллагааг санаатай сулруулах аливаа санаачлагыг хүчтэй эсэргүүцнэ” хэмээн мэдэгдсэн бөгөөд уг мэдэгдлээ бодитоор хэрэгжүүлж Холбооны Мөрдөх Товчооны эсрэг Айпл компаний шүүх ажиллагаанд Айплийг дэмжин оролцсон байна.

Уг хэргийн тухай блогтоо Снапчатын Гүйцэтгэх Захирал Еван Спейгаль бичихдээ Холбооны Мөрдөх Товчоо iPhone утсанд “арын хаалгаар” нэвтрэх эрх олгохыг хүсэж байгаа нь “таны мэдээлэл болон харилцаа холбооны аюулгүй байдал”-д ноцтой аюул заналхийлж байна гэжээ.[141]

Снапчат Айплийн байр суурийг дэмжин арга хэмжээ авсан нь нааштай алхам яах аргагүй мөн бөгөөд шифрлэлтийн “арын хаалгаар” нэвтрэх эрх нь аюултай болохыг олон нийтийн өмнө хүлээн зөвшөөрсөн юм. Гэхдээ компаний олон нийтийн өмнө нээлттэй байдаг бодлогод Засгийн газар эсвэл бусад гуравдагч этгээд нь хэрэглэгчийн хувийн мэдээлэлд нэвтрэх нь хүний эрх, ялангуяа хувийн нууцтай байх, үзэл бодлоо чөлөөтэй илэрхийлэх эрхэд хэрхэн сөргөөр нөлөөлдөг болохыг хүлээн зөвшөөрөөгүй байна.

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Уг шалгуураар Снапчат-д 0 оноо өгчээ.

Snapchat (Снапчат) “Бид маш боловсронгуй шифрлэлттэйгээр бусад сервэртэйгээ харьцдаг ба аюулгүй байдлыг сайжруулахад Кипербичвэр Дамжуулах Протоколын Хамгаалалт буюу HTTPS-г ашигладаг” гэжээ. Үүнээс гадна Снапчат болон бусад нарийн сервэрүүд нь хөдөлгөөнт төхөөрөмж дээр шифрлэгдсэн байна.[142] Энэ үзүүлэлт нь зөөврийн шифрлэлт ашигладаг компани гэдгийг нь харуулж байна. Мөн төгсгөл хоорондын шифрлэлтийг хийдэггүй ба нарийн төвөгтэй нөхцөл байдалд Snapchat (Снапчат)-ын илгээсэн зурвас дахин сэргэх боломжтой байж болох юм.[143]

2016 оны 3-р сард Snapchat (Снапчат)-ыг зурвасийн аюулгүй байдал дээр төвлөрөн ажилладаг гэдгээ мэдэгдсэн байна.[144] Эмнести Интернэшнлд хариу болгож тус компаний мэдэгдэж буйгаар “Бид Снапчат хэрэглэгчдийн аюулгүй байдлыг илүү боловсронгуй болгох шинэ арга замыг үргэлж эрэлхийлдэг ба үүнд төгсгөл хоорондын шифрлэлтийг оролцуулж болох билээ. Гэвч бид бүтээгдэхүүнийхээ онцлогуудыг түгээх боломжгүй” хэмээв. Төгсгөл хоорондын шифрлэлт амжилтгүй болох үед, Снапчат хэрэглэгчдийнхээ хувийн нууцтай байх эрх, үзэл бодлоо илэрхийлэх эрх чөлөөг хангаж чадахаа больдог байна.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести үүнд мөн л 0 оноо өгөөд байна.

Snapchat (Снапчат)-ын хувьд илгээсэн зурвас нь шууд устдаг программтай ба энэ нь хэрэглэгчдэд илгээсэн зурвас нь “түр зуурын” гэх сэтгэгдлийг төрүүлдэг. Гэвч үнэн хэрэг дээрээ тус компаний сервэрт зурвас хэсэг хугацаанд хадгалагдаж байдаг байна. Компани бүрт хэрэглэгчиддээ аюулгүй байдал, хувийн нууцтай байх зэргийн тал дээр ташаа ойлголт төрүүлэх вий гэсэн айдас байдаг. Энэ талаар хэрэглэгчиддээ байнга мэдээлэл өгч, аюулгүй байдлыг хангах нь тэдгээр компаниудын чухал үүрэг хариуцлага юм. Харин энэхүү чухал хүчин зүйлийг шифрлэлтийн тусламжтайгаар хангаж болно.

[140] Snapchat letter, 11 July 2016.
[141] Snapchat, *Why we're standing with Apple*, 3 March 2016, available at: www.snap.com/en-US/news/post/why-were-standing-with-apple/
[142] Snapchat letter, 11 July 2016.
[143] Snapchat Law Enforcement Guide, 16 October 2015, p. 6.
[144] The Guardian, *Facebook, Google and WhatsApp plan to increase encryption of user data*, 14 March 2016.

Снапчатын дотоод аюулгүй байдал нь тухайн веб сайтад мөн холбогдох төхөөрөмжүүдэд хэрэгжих боломжтой.[145] Тус апликейшны үйл ажиллагаа, эсвэл өөр ямар нэгэн зураг авах технологи, screenshot (скрийншот) /дэлгэц дээрх зургийг авах/ зэргийг багтаасан маш өргөн хүрээний мэдээллийг хадгалах, дахин сэргээх зэрэг үйл ажиллагааг тухайн апликейшн-аар хийж болохыг хэрэглэгчддээ дуулгасан билээ. Хэрэглэгчидээсээ гэмт хэрэгтэй холбоотой мөн улсын хяналт шалгалтаар тэдний эрх зөрчигддөгийг нууцалдаг юм. Мөн ямар нэгэн зөвлөмж, заавар өгдөггүй ба хэрэглэгчдийнхээ аюулгүй байдлыг хамгаалахын тулд шифрлэлт хэрхэн хийдэг, ямар төрлийн шифрлэлтийг үйлчилгээндээ ашигладаг талаар ч мөн дэлгэдэггүй байна.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Үүнд Эмнести 3 оноо өгөөд байна.

2015 оны 4-р сараас эхлэн, Snapchat (Снапчат) жилд 2 удаа ил тод байдлын тайланг хэвлэн гаргасаар байна. Үүнд Засгийн газраас хэдэн удаа хэрэглэгчдийн хувийн мэдээллийг авахаар хүсэлт гаргасан талаар нарийн заасан байдаг. 2015 оны 11-р сараас эхлэн, Тус компани нь хэрэглэгчиддээ "Бид хэрэглэгчдийнхээ мэдээлэл рүү нэвтрэх нь хуулиар хориотой зүйл боловч зөвхөн онцгой нөхцөл байдлуудад Жишээ нь: хүний эрх хүчтэй зөрчигдөх, хүүхдийн мөлжлөг, амь насанд нь аюултай байхаар гэмтэж бэртсэн, тохиолдлуудад" зөвшөөрөлгүй нэвтрэхээ сануулсан юм. Эмнести Интернэшнлд хариу болгож Snapchat (Снапчат) "одоогоор Засгийн газраас албан ёсны арын хаалгыг бий болгох тулган шаардалт хүлээн аваагүй байна" хэмээжээ.

Хэрвээ энэхүү шаардлага өмнө нь бидэнд ирсэн бол бид анхнаасаа аюулгүй байдлаа хамгаалах хөтөлбөртөө тусгагдсан зүйлээсээ хойш ухрахгүй байсан тэгэхээр бид тэрхүү шаардлагыг хүлээж авахгүй л гэсэн үг. Эмнести энэхүү байр сууриа зөрчсөн талаарх ямар ч нотолгоо, хэрэглэгчдийн гомдолыг олоогүй юм.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Уг шалгууруар Эмнести Снапчат-д 0 оноо өгчээ.

Өөрийн веб сайт хуудас дээр Snapchat (Снапчат) ямар шифрлэлт хийдэг нь ойлгомжгүй бөгөөд шифрлэлтээ үйлчилгээнд хэрхэн ашигладаг нь ч тодорхой бус байна. Эмнести Интернэшнлийн хариуд тус компани нь зөвхөн "Бид бусад сервэртэй харилцахдаа мөн HTTPS /Кипербичвэр Дамжуулах Протоколын Хамгаалалт/ ашиглахдаа аюулгүй байдлын өндөр түвшний шифрлэлт ашигладаг гэж мэдэгдэв.

ТЕЛЕГРАМ (TELEGRAM)

Телеграм компаний төв нь Холбооны Герман улсад байрладаг ба цахим шууданг хөгжүүлэх, ухаалаг утас мөн бусад төхөөрөмжөөр ашиглахад тохиромжтой шуурхай зурвасын апликейшн юм. Телеграм компаний санхүүгийн дэмжигч Оросын бизнес эрхлэгч Паул Дуров гэгч байдаг ба энэхүү төсөл ажиллагаа нь санхүүгийн зорилтот бус билээ.[146]

2016 оны 2-р сараас эхлэн, сар бүр 100 сая хүний хэрэгцээг хангаж байна гэх тоо баримт гарав.[147] Телеграм нь Эмнестид хариу болгож мэдээлэл хүргүүлсэн болно.

Телеграм бол аюулгүй байдлын цахилгаан холбооны апликейшн хэмээн өөрийгөө дүгнэдэг. Хэрэглэгчдийн хувийн нууцыг хамгаалах тал дээр хүчтэй байр суурь дээр байдаг боловч төгсгөл хоорондын шифрлэлтийг хийдэггүй байна.

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Эмнести Интернэшнл уг шалгуурт 3 оноо өгсөн байна.

---

[145] Snapchat Privacy Policy, available at: www.snapchat.com/privacy
[146] Telegram FAQ telegram.org/faqhow-are-you-doing-to-make-money-out-of-this
[147] TeachCrunch, Encrypte messaging app Telegram hits 100M monthly active users,350K new users each day, 23 Feb 2016

Телеграм нь олон нийтэд баталгаат зурвасын апликейшн гэдгээрээ танигдсан учир нь цахим орчинд хувийн мэдээлэл рүү халдахыг таньж, хэрхэн шифрлэлтийн тусламжтайгаар гаргаж ирдгийг харуулдаг.

Веб сайт дээрээ "бид интернэт орчинд буй хэрэглэгчдийн хувийн мэдээллийг хамгаалах хамгийн чухал 2 бүрэлдэхүүнийг онцолдог: Энэ нь гуравдагч этгээд, эх баригчид, ажилчид гэх зэргээс нууц харилцан яриаг хамгаалах, мөн маркетингийн, зар сурталчилгааны ажилчдаас хувийн мэдээллийг хамгаалах юм.[148]

Хувийн мэдээллийг хэрхэн шифрлэлтийн тусламжтайгаар хамгаалах талаар тайлангаа тавив. Энэ нь веб сайтад эрх чөлөөтэй үзэл бодлоо илэрхийлэх эрхээ хамгаалахыг илэрхийлсэн юм.[149] 2015 оны 11-р сард Парист зэвсэгт халдлага болсонтой холбоотойгоор Телеграмын шифрлэлтийн асуудал маргааны төвд орсон юм.[150] Исламын улс хэмээн өөрсдийгөө нэрлэсэн зэвсэгт бүлэглийн гишүүд ихэвчлэн Телеграмын шуурхай зурвасыг өөр хоорондоо харилцахдаа ашиглаж байсан талаар хэвлэл мэдээллүүд нийтэлсэн юм. Үүнд хариу болгон "Ислам улстай холбоотой гэгдэх олон нийтийн суваг хаасан хэмээнд мэдэгдсэн бөгөөд хувийн нууцтай байх эрхийг хангах үүднээс Дуровын хэлснээр "Хувийн чат нь бидэнд нууц хэвээр үлдэнэ" гэж мэдээлсэн.[151]

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл уг шалгуурт 1 оноо өгчээ.

2013 оны 10-р сараас Telegram (Телеграм) шуурхай зурваст төгсгөл хоорондын шифрлэлийг нэвтрүүлж эхэлжээ. Гэсэн ч төгсгөл хоорондын шифрлэлтийг бүх харилцаа холбоо явагдах үед ашиглах боломжгүй ба харин хэрэглэгчид Secret chat ("Нууц Чат") гэсэн хэсгийг сонгож байж нууцалж болно харин бусад илгээсэн бүх зурвас Cloud chat ("Клауд Чат")-руу шилжих юм. "Клауд Чат" нь хэрэглэгч хоорондоо шифрлэлттэй зурвас илгээнэ гэсэн үг ба Телеграмын үйлчилгээнийхэн энэхүү зурвасны утга кодыг тайлж чадахаар бүтээжээ.

Эмнестид өгсөн хариу захидалдаа Телеграм "Төгсгөл хоорондын шифрлэлтийг бүх хэсэгтээ хийх боломжгүй учир манай компаний хэрэглэгчид "Клауд Чат"-ыг өөрийн нууцлалтай зурвасыг хадгалах, мөн бичиж илгээхдээ ашиглаж болно. Ашигтай тал нь дийлэнхи хэрэглэгчиддээ Apple (Айпл), Google (Гүүгл) зэрэг гуравдагч этгээдийн шийдлүүдийг ашиглах боломжоор хангаж байгаа" гэжээ.

Компаний мэдээллэж буйгаар хэрвээ бүх шуурхай зурвасын апликейшнуудыг "Нууц" гэсэн тодотголтой болговол Клауд чат ашиглагдахаа больж өөр өрсөлдөгч компанид хэрэглэгчдээ алдаж мэднэ хэмээн байр сууриа илэрхийллээ. [152]

Бодит байдал дээр сонголт өгсөн нь аюулгүй байдлыг хангах бодлоготой уялдаж байна. Гэвч Телеграм төгсгөл хоорондын шифрлэлтгүй байгаагаа хүлээн зөвшөөрөх ёстой. Хэрэглэгчиддээ санал болгосон "Нууц Чат" зурвасын апликейшнээ яагаад Телеграм хэрэглэгчиддээ нэг мөр санал болгоогүйг зөвтгөх үндэслэл биш юм. Энэ нь Телеграмыг аюулгүй зурвасын үйлчилгээтэй гэж тодорхойлоход учир дутагдалтай болгож байгаа юм.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести Интернэшнл уг шалгууруар шүүн 1 оноо өгөөд байна.

[148] Telegram,FAQ What your thoughts on intyernet privacy, www.telegram.org
[149] Telegram, FAQ, Do you process take down requests from third parties, telegram.org
[150] See for example:CCN, an app called Telegram is the 'hot new thing among jihadists;17 Nov 2016
[151] Quoted in TechCrunch, after Paris attacks, telegram purges ISIS Public content, 19 Nov 2015, techcrunch.com/2015/11/19/telegram-purges-isis-pubic-channels/
[152] Telegram email to AI 4 Oct,2016

Телеграмын веб сайт дээр байх FAQ [1] буюу тусламж маягаар байх асуулт хариултууд нь энэхүү шифрлэлтийн арга техник, интернэт дэх аюулгүй байдлыг хангах харьцангуй шинэ арга барил гэдгийг тайлбарласан байна. Мөн энэхүү "Нууц чат" гэх хэсэгрүү өөрсдөө ч нэвтэрч чадахааргүй зохион бүтээжээ.[153] Энэ апликейшн нь төгсгөл хоорондын шифрлэлтээр кодлогдсон байдалтай ба энэ апликейшныг бусад хэлбэрийн чатаас онцлохын тулд ногоон өнгөөр цоожны зурагтай хамт харагдахаар бүтээжээ.

Тус компани нь тийм ч өндөр хамгаалалт бүхий бус шифрлэлттэй "Клауд Чат" апликейшныг ашиглах явцад хэрхэн хэрэглэгч нар эрсдэлтэй тулгардаг талаар сануулга өгөөгүй юм. Энэ нь ямар асуудлыг үүсгэж байна вэ гэхээр энэхүү апликейшн нь хэрэглэгчдэд өндөр чанар бүхий шифрлэлт хийгдсэн гэсэн таамаглалыг үүсгэж байгаа юм.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Үүнд Эмнести 2 оноо өгөөд байна.

Телеграмын дотоод бодлого нь маш энгийн "хэнд ч мэдээллийг ил болгохгүй" гэсэн байдаг. Харин Эмнестид өгсөн хариундаа "Ямар нэгэн мэдээллийг хадгалж хамгаалахдаа бид шифрлэлийг хэрэглэдэггүй харин яг хэрэгтэй нөхцөл байдал дээр ашигладаг. Клауд Чатын мэдээлэл нарийн бүтэц бүхий өөр өөр улс, нутаг дэвсгэрт байх сервэрт хадгалагддаг. Холбогдох код тайлах аргууд нь хэдэн хэсэгт хуваагддаг ба эдгээр нь хадгалсан мэдээллүүд шигээ нэг өөр өөр газар нутагт, янз бүрийн шүүхийн тогтолцоонд хамаарах хуулийн этгээдүүдийн хяналтан доор байдаг" гэжээ.

Хувийн нууцтай байх эрх, үзэл бодлоо чөлөөтэй илэрхийлэх эрх чөлөөнд халдаж чадах боломжийг ямар ч үед хэнд ч олгохгүй нь маш гайхалтай бүтэц, зохион байгуулалтын үр дүн билээ. Хэрвээ хэзээ нэгэн цагт биднээс мэдээлэл шаардвал тэдгээр нөхцөл байдал нь заавал маш чухал, мөн дэлхийн хэмжээний хууль ёсны хяналт шалгалтаар орсон байх болно гэв."[154] Энэ нь Телеграм компани цөөн хэдэн тохиолдолд л хэрэглэгчдийнхээ хувийн мэдээллийн талаар Засгийн газар, батлан хамгаалах байгууллагуудад хүргэдэг гэсэн үг болж байна. Мөн тухайн компани нь Засгийн газар зэрэг гуравдагч этгээдүүдэд хэрэглэгчдийнхээ 0 байт мэдээллийг өгөхийг зөвшөөрдөг байна.[155] Тэд Засгийн газраас хүлээн авсан мэдээллийг өгөх хүсэлтийг тэр бүр нарийвчлан олон нийтэд мэдэгддэггүй. Энэ тохиолдолд хэрхэн ямар мэдээллийг аль хүнээс хэзээ хэдэн удаа авахаар хүсэлт гаргасан талаар бүх мэдээллийг хэрэглэгчид өөрт нь мэдээллэх ёстой байдаг. Эмнестид өгсөн хариундаа Телеграм нь: "Бид хэрэглэгчдийн мэдээлэлд арын хаалга гаргаж оруулахгүй, цаашид ч ийм явдал гаргуулахгүй байхыг баталж чадна" гэв.

Зарим улс орнуудад нэвтрүүлж байгаа шифрлэлтийн эсрэг хуулийг бид эсэргүүцэж байгаа бөгөөд бид сервэр рүүгээ нууцаар хэн нэгнийг нэвтрэхийг хэзээд эсэргүүцсээр байна гэж Телеграм мэдэгдсэн юм.[156] Эмнести тэднийг энэхүү байр сууриа зөрчсөн ямар ч нотолгоо, хэрэглэгчдийн санал хүсэлтийг олоогүй юм.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Уг шалгуураар Эмнести Телеграмд 3 оноо өгчээ.

Энэхүү шалгуурт тус компанийг "өндрөөр" үнэллээ.
Телеграм бүрэн нээлттэй эх сурвалжийн хувьд шифрлэлтийн протокол хэрэглэдэг.[157] Нэг томоохон шүүмжлэл дагуулах зүйл бол тэд "Гар хийцийн нууц бичээс тайлалтын шифрлэлт" ба өөрсдөө нууц бичээс тайлалтын протокол зохион бүтээн хэрэглэдэгт байгаа юм.

[153] Telegram, Secret Chats, telegram.org/privacysecret-chats
[154] Telegram email to AI 28 July,2016
[155] Telegram, Do you process data requests?, telegram.org/faq/q/do-you-process-data-requests
[156] Telegram email to AI 28 July,2016
[157] The Atlantic, the Flaw in ISIS's Favorite Messaging App, 4 Jan 2016J.Jakobsen and C.Orlandi Aarhus Universit, on the CCA (in) security of MT Proto, 8 Des 2015, last revised 31 Mar 2016,eprint.iacr.org/2015/1177

Нууц бичээс тайлалтыг хэрэглэх нь стандарт протоколд зааснаар аюулгүй байдлыг хангалттай хангаж үл чадна мөн үүнийг нь ч олон нийт хүлээн зөвшөөрсөн байдаг. Өнөөг хүртэл Телеграмын дотоод аюулгүй байдалд халдаж ороход тийм ч амар хялбар байгаагүй ба бид энэхүү байдлаа хадгалж улам бүр хамгаалалтаа сайжруулахын тулд аюулгүй байдлыг мэргэжилтнүүд,[158] энэхүү асуудал хариуцсан хөгжүүлэгчидтэй тууштай хамтарч үргэлжлүүлэн ажиллахаа мэдэгджээ.[159]

TENCENT (ТЕНСЭНТ)

БНХАУ-д 2 алдартай зурвасын апликейшн байдгийн нэг нь WeChat (Вичат) "Weixin in China" нэрээрээ илүү танигдсан харин нөгөө нь "QQ" (Кю Кю) Мессэнжир, эдгээрийн хөгжүүлэгч компани бол Тенсэнт билээ.[160] Тенсэнт-ийн мэдээлэж буйгаар сар бүр /Вей шин in China/ Ви Чат 697 сая хүн дэлхий даяар идэвхитэй хэрэглэгч харин QQ чат нь 853 сая хэрэглэгчтэй байдаг хэмээв.[161]

Ви Чат бол Хятад улсад хамгийн өргөн хэрэглээг хамарсан ба дан ганц зурвас илгээх биш хоол, хүнс зэрэг хэрэглээний мөнгө тушаах, хүргэлт, захиалах, тоглох гээд хэд хэдэн үйлдлийг хийх чадвартай апликейшн билээ.[162] Тенсэнт Эмнестид хариу захиа илгээгээгүй нь ерөнхийдөө холбоо харилцаа тааруу зарим асуудал, хүний эрхийн тал дээр ямар нэгэн мэдээлэл хийдэггүй нь нотлогдсон юм. Мөн тийм ч боловсронгуй шифрлэлт хэрэглэдэггүй нь харагддаг. Гэвч Хятад улсын Засгийн газар Цахим орчинд хяналтыг маш чанд барьдаг боловч хууль ёсны гэж хүлээн зөвшөөрөгдөх нь маш хүндрэлтэй байдаг байна.

2015 оны 7-р сард нэгэн иргэн We Chat "Ви Чат" Хятад улсын нөлөө бүхий хүмүүс блог, вебүүдийн нийтлэх зүйлст хязгаарлалт, хяналт тавьдаг талаар мэдээлэв.[163] Энэ явдал хэд хэдэн жишээн дээрээс харагддаг ба улс төрийн гол байр суурь бол бичиг зохиол түүн дээр хяналт, ажиглалт хийхэд төвлөрдөг. [164]

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Эмнести Интернэшнл уг шалгуурт 0 оноо өгсөн байна.

Tencent (Тенсэнт) компани нь Хятад улсад, тэнд оршин суугаа иргэдийн, дэлхий нийт хүмүүсийн хувьд нээлттэй бодлого баримтлан үйл ажиллагаагаа WeChat (ВиЧат), QQ Messenger (КЮ КЮ мессэнжир)-г ашиглан явуулж байна. Энэхүү 2 апликейшны бодлогыг хувийн аюулгүй байдлыг хангадаг[165] гэдэг хэдий ч хэрэглэгчдэд үзэл бодлоо илэрхийлэх эрх чөлөөг олгодоггүй байна.

Хэрэглэгчдийн эрхийг хамгаалсан яг ямархуу арга хэрэгсэл хэрэглэдэг талаарх нь тийм ч тодорхой биш ба тэдний тайлбарлаж буйгаар "бид маш өндөр технологи бүхий аюулгүй байдлын процедурыг ашигладаг ба энэхүү аргыг ашиглаж байхад буруугаар урвуулан ашиглах, хэрэглэгчдийн хаяг руу нэвтрэх, мэдээлэл алдагдах зэрэг асуудал гарахгүй" хэмээн тайлбарлаж байгаа юм.[166] Тенсэнт нийгмийн хариуцлагатай таван корпорацитай хэдий ч хэрэглэгчийн хувийн мэдээлэл эсвэл үзэл бодлоо илэрхийлэх эрх чөлөөнд халдах зэргийг алийг ч хүлээн авч үздэггүй байна. Бидний асуултад хариу өгөөгүй ба бид хэрэглэгчдийнхээ эрхийг хамгаалах бодлого хэрэгжүүлж байсан гэх нотолгоо олдоогүй юм.

---

158 Cybersecurity expert B. Schneier, Amateurs Produce Amateur Cryptography, 12 May 2015, available at: www.schneier.com/blog/archives/2015/05/amateurs_p roduc.html
159 Telegram email to Amnesty International, 4 October 2016.
160 China Internet Watch, Top 6 China mobile social networking apps, 1 April 2016.
161 Tencent, About Tencent, available at: www.tencent.com/en-us/at/abouttencent.shtml
162 The Financial Times, Overloaded China users battle 'WeChat fatigue', 16 April 2016.
163 J. Q. Ng, University of Toronto's Citizen Lab, Politics, Rumors, and Ambiguity: Tracking Censorship on WeChat's Public Accounts Platform, 20 July 2015, available at: https://citizenlab.org/2015/07/tracking-censorship-on-wechat-public-accounts-platform/
164 J. Q. Ng, University of Toronto's Citizen Lab, *Politics, Rumors, and Ambiguity: Tracking Censorship on WeChat's Public Accounts Platform, 20* July 2015, Appendix: Documented Cases of WeChat Restrictions.
165 Tencent Privacy Policy (outside China), available at: www.tencent.com/en-us/zc/privacypolicy.shtml; Tencent Privacy Policy for users within China and Chinese citizens, available at: www.qq.com/privacy.htm
166 Tencent letter to Business and Human Rights Resource Centre, 2015, available at: https://business-hurnanrights.org/en/tencent-0

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл уг шалгуурт 0 оноо өгчээ.

Зөөврийн шифрлэлтийг Ви Чат-д нэвтрүүлсэн ч гэлээ хэрэглэгч ажилтан хоорондын харилцаа холбоо нь нягт биш мөн төгсгөл хоорондын шифрлэлт хийгдээгүй.[167] Эмнести Интернэшнл QQ (КюКю) мессенжэрийн шифрлэлтийн талаарх мэдээллийг олоогүй юм. 2016 оны 3-р сард БНХАУ-ын иргэд мэдэгдсэнээр Тенсэнтийн өөр нэг QQ Browser (Бровсэрт) нэвтрэн орж нууцлалыг тайлахад маш амархан гэв. [168]

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести Интернэшнл уг шалгууруар шүүн 0 оноо өгөөд байна.

Дээр дурдсанчлан Тенсэнт тодорхой хязгаарлалт бүхий мэдээллээр тэрхүү нэвтрэн орсон гуравдагч этгээдийг хангадаг байна. Харин Ви Чатын олон улсын веб-сайт дээр FAQ хамгаалалтыг ашигладаг ба түүнд л шифрлэлтийн талаарх хэдэн үндсэн мэдээлэлүүд байдаг байна.[169] Дээрх хоёр мессенжэрийн апликейшнд бүртгүүлэх үед тус компаний дотоод аюулгүй байдлын бодлоготой холбоотой холбоос гарч ирдэг ч тус апликейшнуудыг хэрэглэж байх явцад шифрлэлтийн талаар, мөн дотоод аюулгүй байдлын бодлоготой холбогдох холбоос байдаггүй.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Үүнд Эмнести бас 0 оноо өгөөд байна.

Тенсэнтийн Олон улсын Хувийн мэдээллийн талаарх баримт “манай салбар компаниуд хэрэглэгчдийн хувийн мэдээллийг задлах, хадгалах, сэргээх зэргийг шаардуулж болно” гэдэг зүйлийг онцолдог. Гэхдээ зөвхөн доорх шаардлага тулгарсан тохиолдолд билээ. (I.) хүчин төгөлдөр хууль, дүрмийг биелүүлэх зорилгоор; (II.) шүүхийн шийдвэр, шүүхэд зарлан дуудах хуудас, бусад хуулийн заалтуудыг биелүүлэх зорилгоор; (III.) Засгийн газар, батлан хамгаалах агентлагууд, үүнтэй адил байгууллагуудын хүсэлтэд хариу болгон өгөх; (IV.) Дагаж мөрдөх шаардлагатай хууль, дүрмүүдээр хүлээн зөвшөөрсөн тохиолдолд; Тухайн компани нь хэрэглэгчиддээ хэрхэн тэдний мэдээллийг авах зорилгоор хүсэлт ирсэн тухай мэдээлэл хийдэггүй. Мөн Эмнести шифрлэлттэй холбоотой нууц нэвтрэх арга зэргийг олох боломж байгаагүй билээ.[170]

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Уг шалгууруар Эмнести Тенсэнт-д 0 оноо өгчээ.

Дээр гарснаар Эмнести 2 апликейшнд хэрэглэж буй шифрлэлтийн талаар нарийн мэдээлэл олж чадаагүй байна.

Viber Media (Вайбер Мэдиа)

Viber Media (Вайбер Медиа) бол гар утас, бусад төхөөрөмжөөр ашиглаж болох ба текст, бичлэг, зураг тавих, дуу хоолой, бичлэг хийж болох шуурхай зурвасын апликейшн юм.

---

[167] Tencent, How secure are my chat messages and conversations on WeChat? Can third parties snoop or read my messages?, available at: https://help.wechat.com/cgi-bin/micromsgbin oshelpcenter?opcode=2&plat=1&lang=en&id=1208117b2mai1410243yyQFZ&Channel=helpcenter
[168] J. Knockel, A. Senft, R. Deibert, Citizen Lab, WUP! There It Is: Privacy and security issues in QQ browser, 28 March 2016, available at: https://citizenlab.org/2016/03/privacy-security-issues-qq-browser/
[169] Tencent, How secure are my chat messages and conversations on WeChat? Can third-parties snoop or read my messages?
[170] Tencent Privacy Policy (International).

Люксенбург улсад үүсгэн байгуулагдсан ба төв оффис нь Израйль улсад байрладаг. Япон улсын Ракутен интернэт компани нь охин компаниар үйл ажиллагаагаа явуулдаг байна. [171] Viber (Вайбер) үйлчилгээг 700 сая хүн хэрэглэдэг ба 250 сая хүн өдөр тутамдаа идэвхтэй хэрэглэдэг байна. Эмнести-д хариу болгож мэдээлэл илгээсэн болно.[172]

ШАЛГУУР ҮЗҮҮЛЭЛТ 1: КОМПАНИ НЬ БОДЛОГО, ҮЙЛ АЖИЛЛАГААГААРАА ДАМЖУУЛАН ХЭРЭГЛЭГЧДИЙНХЭЭ ХУВИЙН НУУЦТАЙ БАЙХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨГ ЭРСДЭЛД ОРУУЛАХ ЦАХИМ ХАЛДЛАГЫГ ОЛЖ ТОГТООДОГ УУ?

Эмнести Интернэшнл уг шалгуурт 1 оноо өгсөн байна.

Эмнести-д өгсөн хариудаа “Viber (Вайбер) нь хэрэглэгчдийнхээ эрхийг хамгаалахдаа “номер 1” хэмээв.

Хамгаалалт, шифрлэлтийг хэрэглэн аюулгүй байдлаа хангах бодлого хэрэглэдэг хэдий ч Эмнести хэрэглэгчдийн эрхийг хамгаалах бодлого хэрэгжүүлж байсан гэх нотолгоо олдоогүй юм. Тус апликейшн нь хэрэглэгчдийн үзэл бодлоо илэрхийлэх эрх чөлөөтэй холбоотой ямар нэгэн үүрэг хүлээгээгүй. Хэрэглэгчдийн эрхийг хамгаалсан, хүний эрхийг зөрчиж буй байдлыг багасгах түүнээс хамгаалах яг ямархуу арга хэрэгсэл хэрэглэдэг талаарх нь тодорхойгүй байна.

ШАЛГУУР 2: КОМПАНИ НЬ ТӨГСГӨЛ ХООРОНДЫН ШИФРЛЭЛТИЙГ АВТОМАТААР ХЭРЭГЖҮҮЛДЭГ ҮҮ?

Эмнести Интернэшнл уг шалгуурт 3 оноо өгчээ.

2016 оны 4-р сараас хойш Viber Media (Вайбер Медиа) төгсгөл хоорондын шифрлэлтийг бүрэн хэрэгжүүлж эхэлсэн гэдгээ зарлажээ. Бүх төрлийн чат-д төгсгөл хоорондын шифрлэлтийг ашигладаг ба программын нэгд хуучин хувилбарыг ашиглаж байна. Суурин утас, гар утасруу залгахдаа интернэт ашиглаж болох Viber out “Вайбер аут” үйлчилгээндээ төгсгөл хоорондын шифрлэлтийг ашигладаггүй байна.

ШАЛГУУР 3: КОМПАНИ НЬ ХУВИЙН НУУЦЛАЛАА АЛДАХ, ҮЗЭЛ БОДЛОО ИЛЭРХИЙЛЭХ ЭРХ, ЭРХ ЧӨЛӨӨ НЬ ХАЛДЛАГАД ӨРТӨЖ БОЛОХ ТАЛААР ХЭРЭГЛЭГЧДЭДЭЭ МЭДЭГДДЭГ ҮҮ? ҮҮНИЙГ ШИФРЛЭЛТИЙН ТУСЛАМЖТАЙГААР ХЭРХЭН ШИЙДВЭРЛЭДЭГ ВЭ?

Эмнести Интернэшнл уг шалгууруар шүүн 1 оноо өгөөд байна.

Вайбер FAQ хамгааллатыг хэрэгжүүлж хэрэглэгчдэд хэрхэн ажилладаг, шифрлэлт зэргийн талаар мэдээлэл өгдөг. Тухайн апликейшндаа зурвас, харилцан яринд түвшин бүрийн шифрлэлт хэрэглэсэнээ өнгөт цоожны дүрсийг ашиглан харуулахаар системчилсэн. Гэхдээ энд сул шифрлэлт гэдгийг илтгэх сануулга байхгүй. Мөн төгсгөл хоорондын шифрлэлт хэрхэн хэрэглэгдсэн, утасны интернэттэй хэрхэн холбогдож буй талаар нарийн ойлголт өгөгдөөгүй.

Иймд тэд хэрэглэгчиддээ эрх нь хэрхэн алдагдаж буй талаар мэдээллэх боломжгүй ба тэд хариу болгож “засгийн газар энэ төрлийн асуудлыг улам нэмэгдүүлж байгаа”-тай санал нэг байгаагаа илэрхийлэв. Гэхдээ тус компани Засгийн газраас хяналт тавьж буйг хэрэглэгчиддээ дэлгэдэггүй байна.

ШАЛГУУР 4: ХЭРЭГЛЭГЧИЙН МЭДЭЭЛЛИЙГ ДАМЖУУЛАХ ЗАСГИЙН ГАЗРЫН ХҮСЭЛТИЙГ ОЛОН НИЙТЭД ИЛ БОЛГОДОГ ЭСЭХ? ЯМАР ХАРИУ АРГА ХЭМЖЭЭ АВДАГ ВЭ?

Үүнд Эмнести бас 1 оноо өгөөд байна.

Тус компани мэдээллийг нь хүлээн авах зорилгоор Засгийн газраас хүсэлт ирсэн тухай хэрэглэгчиддээ мэдэгдэггүй.

---

[171] Rakuten website, available at: http://global.rakuten.com/corp/about/company/digital.html
[172] Viber letter to Amnesty International, 12 July 2016 (Viber letter); Statista, Leading social networks worldwide as of September 2016, ranked by number of active users.

Засгийн газар, батлан хамгаалах байгуулагуудад маш чухал шаардлагатай гэсэн тохиолдолд буюу улсын аюулгүй байдлын төлөө хэрэглэгчдийнхээ хувийн мэдээллийг хүргэдэг байна. Гэхдээ тухайн хэрэглэгчдэд мэдээлэх үгүйгээс үл хамаардаг. Үүнийгээ Засгийн газар өөрөө манай апликейшн руу нэвтрэн орохгүй байлгах арга хэмээсэн байдаг.[173] 2016 оны 4-р сард нууцаар нэвтрэн орохыг ямар ч нөхцөлд хүлээн зөвшөөрөхгүйгээ мэдэгдсэн.[174] Энэхүү хэлсэн амлалтаа зөрсөн тохиолдол одоогоор байхгүй байна.

ШАЛГУУР 5: КОМПАНИ НЬ ӨӨРИЙН ШИФРЛЭЛТИЙН СИСТЕМИЙН ТАЛААРХ ТЕХНИКИЙН ДЭЛГЭРЭНГҮЙ МЭДЭЭЛЛИЙГ НИЙТЭЛДЭГ ЭСЭХ?

Уг шалгууураар Эмнести Тенсэнт-д 1 оноо өгчээ.

Апликейшндаа хэрхэн шифрлэлт ашигладгаа ерөнхийгөөр тоймлон үзүүлдэг.[175]

Viber (Вайбер) мэдээлэхдээ тус протоколыг нээлттэй шивнээ гэх апликейшнд ашигладаг "давхар ратчет" протоколтой адил ойлголтоор ашигладаг.

Гэхдээ шифрлэлтийн протокол бол нээлттэй эх сурвалж биш билээ. Энэхүү шүүмжлэлд хариу болгож “бидний шифрлэлтийн протокол бол нээлттэй эх сурвалж дээр үндэслэж байгаа ба дотоод аюулгүй байдлаа нэмэгдүүлсэн нэмэлт түвшинтэй” гэсэн хариуг Эмнестид хүргүүлсэн юм.[176]

[173] Viber letter 12 July,2016
[174] Techcrunch, Viber defends new end-to-end encryption protocol against critism, 20 April 2016 techcrunch.com/2016/04/20/viber-defends-new-end-to-end-encryption-protocol-against-critism/
[175] Viber Encryption Overview,available at: www.viber.com /en/security-overview
[176] TechCrunch, *Viber defends new end-to-end encryption protocol against criticism*, 20 April 2016.

ЭМНЕСТИ ИНТЕРНЭШНЛ БОЛ ХҮНИЙ ЭРХИЙН ТӨЛӨӨХ ДАЯН ДЭЛХИЙН ХӨДӨЛГӨӨН.

НЭГ Л ХҮНИЙ ЭРХ ЗӨРЧИГДВӨЛ ЭНЭ НЬ БИД БҮГДЭД ХАМААТАЙ.

Холбоо барих

info@amnesty.org
mongolia.amnesty@gmail.com

+44 (0)20 7413 5500
+976 7000 4708

www.facebook.com/AmnestyGlobal
www.facebook.com/ Amnesty International Mongolia - Монголын Эмнести Интернэшнл

@AmnestyOnline

ГАНЦХАН ЧИ УНШДАГ ГЭЖ ҮҮ?

ХҮНИЙ ЭРХ БОЛОН ШИФРЛЭЛТТЭЙ ХОЛБООТОЙ АСУУДЛААР ТЕХНОЛОГИЙН 11 КОМПАНИЙГ ҮНЭЛСЭН НЬ

Шифрлэлт нь цахим орчинд байгаа хүмүүсийн эрхийг хамгаалдаг ба цахим ертөнцийн орчинд илгээгдсэн хувийн мэдээллийн аюулгүй байдлыг хангадаг. Мөн тухайн орчинд ямар нэгэн айдасгүйгээр өөрсдийн үзэл бодлоо чөлөөтэй илэрхийлэх боломжийг хүмүүст олгодог.

Шифрлэлт нь бидний хувийн мэдээллийг хулгайлах цахим гэмт хэргүүдийг таслан зогсоож, бидний харилцаа холбоог хууль бусаар хянах Засгийн газрын үйл ажиллагаанаас урьдчилан сэргийлэхэд тусалдаг. Ялангуяа энэ нь Хятадын тэрс үзэлтнүүд, нутгаасаа дайжсан Бахрейны идэвхтнүүд, Европын эрэн сурвалжлах сэтгүүлчид зэрэг дэлхий дахинд байгаа хүний эрхийн хамгаалагчид, сэтгүүлчдийн хувьд чухал ач холбогдолтой юм. Мэдээллийн аюулгүй байдлын зөрчил нь тэдгээр хүмүүсийн амин чухал ажлыг үгүй хийж, цаашлаад баривчлагдан саатуулагдах шалтгаан болж болзошгүй. Тоон мэдээллийн аюулгүй байдлын бат бөх чанарыг хадгалахад технологийн компаниуд чухал үүрэг хүлээдэг.

Энэ тайланд өөрсдийн хэрэглэгчдийн цахим аюулгүй байдлыг хамгаалахад ашиглаж буй шифрлэлт нь хүний эрхийн хүлээсэн үүрэгтэй нь нийцэж байгаа эсэхийг харуулсан 11 компаниудын жагсаалтыг авч үзсэн. Үүнд дэлхийн сая сая хүмүүсийн өдөр тутмын харилцаа холбоондоо ашигладаг Скайп (Skype), ВатсАпп (WhatsApp), ВиЧат (WeChat) зэрэг шуурхай зурвасын үйлчилгээ үзүүлэгчдийг хамруулсан болно.

Эмнести Интернэшнл дэвшилтэт технологийн бүх компаниас төгсгөл хоорондын шифрлэлтийг мессенжэрийн үйлчилгээндээ нэвтрүүлсэн үү? хэмээн асуусан билээ. Мөн компаниуд бүгд хэрэглэгчдийнхээ хувийн нууцтай, үзэл бодлоо чөлөөтэй илэрхийлэх эрх, эрх чөлөөг хамгаалах тал дээр илүү анхааран ажиллах хэрэгтэйг ойлгууллаа.

ИНДЕКС: POL 40/4985/2016
2016 ОНЫ 10 САР
ХЭЛ: АНГЛИ
amnesty.org

ЭМНЕСТИ ИНТЕРНЭШНЛ