فری ٹو پروٹیسٹ
گائیڈ پاکستان

فری ٹو پروٹیسٹ گائیڈ پاکستان

پاکستان کے قوانین اور پالیسیوں کے مطابق، مقامی سماجی کارکنوں اور پرائیویسی انٹرنیشنل کے تعاون سے'' فری ٹو پروٹیسٹ گائیڈ'' یو۔کے کو رہنما خطوط کے طور پر تصور کرتے ہوئے بنائی گئی ہے۔اس گائیڈ کا مقصد قانونی مشورے کے متبادل کے طور پر نہیں ہے بلکہ یہ آزاد اور محفوظ طریقے سے احتجاج کے حق کی حفاظت اور مقامی سماجی اور سیاسی کارکنان کی معلومات اور ترجیح کو پیش کرنا ہے۔

گائیڈ کا لنک :
https://privacyinternational.org/sites/default/files/2021-06/FREE_TO_PROTEST-UK-EDITION.pdf

قانون کیا کہتا ہے؟

احتجاج کے حق کو دنیا بھر میں بنیادی جمہوری آزادی کے طور پر تسلیم کیا جاتا ہے۔ پاکستان ایک جمہوری ملک کے طور پر اپنے شہریوں کے اس حق کو تسلیم کرتا ہے۔ اسلامی جمہوریہ پاکستان 1973 کے آئین کا آرٹیکل 16 (بطور ترمیم شدہ) ہر شہری کو یہ حق دیتا ہے کہ ''امن و امان کے مفاد میں قانون کی طرف سے عائد کردہ کسی بھی معقول پابندی کے ساتھ، پرامن طریقے سے اور بغیر ہتھیاروں کے جمع ہو کر احتجاج کر سکتے ہیں۔''
تاہم، پاکستان کے آئین کے آرٹیکل 16 اور 17 کے تحت اسمبلی اور ایسوسی ایشن کی آزادیوں پر ریاستی قانون کے مطابق "مناسب پابندیاں" لگائی جا سکتی ہیں جسے '' پبلک آرڈر'' کا نام دیا گیا ہے۔
اس استثنیٰ کے تحت، مینٹیننس آف پبلک آرڈر آرڈیننس، 1960 جیسے قوانین کا استعمال عوامی اجتماعات کو روکنے اور مظاہرین کو گرفتار کرنے کے لیے کیا جاتا ہے۔
ضابطہ فوجداری (سی آر پی سی) 1973 کی مزید دفعہ 144 کا استعمال 5 سے زائد افراد کے اجتماعات کو روکنے کے لیے بھی کیا گیا ہے تاکہ
قانونی طور پر ملازمت کرنے والے کسی بھی فرد کو رکاوٹ، جھنجھلاہٹ یا چوٹ، یا انسانی جان، صحت یا حفاظت'' کو ''خطرہ، یا عوامی سکون میں خلل ڈالنا، یا ہنگامہ آرائی کی وجہ سے مشکلات کا سامنا نہ ہو۔''
پاکستان انسانی حقوق کے متعدد بین الاقوامی معاہدوں کا بھی دستخط کنندہ ہے اور اس کے مطابق ان معاہدوں کے اصولوں اور قواعد کو برقرار رکھنے کا ذمہ دار بھی ہے۔
خاص طور پر قابل غور بات یہ ہے کہ پاکستان 1966 کے شہری اور سیاسی حقوق کے بین الاقوامی معاہدے کا ایک ریاستی فریق ہے اور اس نے 2010 میں اس معاہدے کی توثیق کی تھی۔ اس بارے میں میثاق کا آرٹیکل 21 کہتا ہے کہ: **(ICCPR)**

پرامن اجتماع کے حق کو تسلیم کیا جائے گا۔اس حق کے استعمال پر کوئی پابندی نہیں لگائی جا سکتی سوائے قانون کے مطابق عائد کردہ پابندیوں کے جو کہ ایک جمہوری معاشرے میں قومی سلامتی یا پبلک آرڈر (آرڈر پبلک)، عوام کے تحفظ، صحت یا اخلاقیات یا دوسروں کے حقوق اور آزادی کے تحفظ کے مفاد میں ضروری ہیں۔

یہ گائیڈ کسی بھی طرح کے ایسوسی ایشن اور اسمبلی کی آزادی کے اور حق کے استعمال کو آسان بنانے کے لیے بنائی گئی ہے ۔ ہماری خاص توجہ کا مرکز یہ ہے کہ احتجاج کا حق استعمال کرنے والے کسی بھی شہری کی رازداری اور ڈیٹا کو لاحق خطرات کو کم کر کے محفوظ کرنے میں یہ گائیڈ مددگار ثابت ہوسکے۔ہم امید کرتے ہیں کہ درج ذیل باب ان کو کچھ

خطرات اور تخفیف(کسی چیز کو کم ناگوار بنانا) کے اقدامات کو واضح کرنے میں مدد کرے گا، جو شہری اپنی آئینی آزادیوں کو استعمال کرنے کا انتخاب کرتے ہیں۔

ہماری کوشش یہ ہے کہ یہ گائیڈ ایک ایسی دستاویز ہو جو موجودہ حالات اور ہر طرح کے آنے والی صورتحال اور دباؤ کے ساتھ ساتھ تبدیل اور بہتر ہو سکتی ہےاور اس مقصد کے لیے ہم گائیڈ میں متعلقہ تبدیلیاں اور اضافے کرنے کے بارے میں کوئی بھی رائے حاصل کرنے کے منتظر ہیں اس کے لیے براہ کرم اپنی بات یا نقطہ **info@privacyinternational.org** پر سبجیکٹ لائن ''پاکستان احتجاج گائیڈ'' کے ساتھ بھیجیں۔

احتجاج میں شرکت سے پہلے اور اس کے دوران دوسرے کارکن کیا کر سکتے ہیں اس کے بارے میں کچھ عمومی نکات یہ ہیں:

۱) ہائیڈریشن کے لیے پانی کی ایک بوتل ساتھ لے جائیں۔ آنسو گیس کے استعمال کی صورت میں اپنی آنکھوں کو اچھے طریقے سے دھوئیں۔

۲) ''بڈی سسٹم'' کو استعمال کریں۔ اگر پولیس پہنچ کر ہجوم کو منتشر کرنے یا کسی اور طریقے سے احتجاج میں خلل ڈالنے کی کوشش کرے تو اس بات کو یقینی بنانا ہے کہ الجھاؤ یا بھگدڑ کی صورت میں کوئی بھی پیچھے نہ رہ جائے۔

۳) احتجاج کے لیے نکلنے سے پہلے اپنے فون کو مکمل طور پر چارج کر کے رکھیں اور کسی عزیز کے ساتھ اپنی لوکیشن شیئر کریں۔

۴) اپنے فون پر پاس کوڈ کو آن کریں کسی بھی چہرے یا فنگر پرنٹ ان لاک کے طریقے کو کو آف کر دیں۔
احتجاج کے لیے اپنے ساتھ حساس معلومات پر مشتمل آلات نہ لائیں۔

۵) اپنے آپ کو گندگی اور آلودگی سے بچانے کے لیے ماسک پہنیں اور اگر کوئی تصویر یا ویڈیوز ریکارڈ کر رہا ہو تو اس کی مدد سے اپنے چہرے کو کم آویزاں کرنے میں بھی مدد کریں۔

۶) تصاویر یا ویڈیوز لے کر پولیس کی طرف سے کی جانے والی کسی بھی چوٹ کا ریکاڈر دستاویز کی صورت میں کریں۔

۷) ساتھی مظاہرین کی تصاویر سوشل میڈیا پر شیئر نہ کریں تاکہ ان کی موجودگی کی نشاندہی نہ ہو۔اس کے بجائے آپ دھندلے چہروں والی تصاویر استعمال کر سکتے ہیں۔

۸) اپنے اور اپنے ساتھیوں کے لیے احتجاج کے اہاتے سے باہر نکلنے کی حکمت عملی پہلے سے طے کریں۔

انٹرنیٹ یا نیٹ ورک شٹ ڈاؤن کو روکنا :

انٹرنیٹ بند ہونے کی صورت میں کیا کیا جا سکتا ہے:

ڈالنے کا ایک عام ذریعہ بن گیا ہے۔ انٹرنیٹ میں انتشار[2] انٹرنیٹ اور موبائل نیٹ ورکس میں خلل بدقسمتی سے مظاہروں[1] کی بندش نہ صرف لوگوں کی آزادیوں کو متاثر کرتی ہے، بلکہ کسی بھی مظاہرے میں گھبراہٹ یا ہلچل کی صورت میں مظاہرین کے لیے مواصلات کو مسدود کرنے کے سنگین نتائج ہو سکتے ہیں۔پاکستان میں انٹرنیٹ کی بندش کو مبینہ طور پر بڑے پیمانے پر اجتماعات اور احتجاج کو کنٹرول کرنے کے لیے استعمال کیا جاتا رہا ہے۔حکومت اکثر موبائل نیٹ ورکس کو بند کرنے کے لیے پاکستان ٹیلی کمیونیکیشنز (ری آرگنائزیشن) ایکٹ 1996 کے سیکشن 54(3) کا استعمال کرتی ہے۔ ذیلی

---

[1] Imran Asghar, "No mobile, internet service today," The Express Tribune, March 23, 2022, https://tribune.com.pk/story/2349211/no-mobile-internet-service-today.

[2] Muneeb Ahmad, "Mobile services to remain suspended in 52 cities on Muharram," TechJuice, October 10, 2021, https://www.techjuice.pk/mobile-services-to-remain-suspended-in-52-cities-on-muharram/.

دفعہ میں کہا گیا ہے کہ صدر کی طرف سے ایمرجنسی کے اعلان پر پی ٹی اے ایکٹ کے تحت کسی بھی لائسنس کو معطل کر سکتا ہے یا اس میں ترمیم کر سکتا ہے یا آپریشن، کام یا سروس کی معطلی کا سبب بن سکتا ہے۔

نیٹ ورک بلاک کرنے کے اثرات کو کم کرنے کے لیے ایپ پر مبنی کچھ مواصلات یہ ہیں:

Fire Chat
ایک ایسی ایپ ہے جو پیغامات کے تبادلے کے لیے بلوٹوتھ کا استعمال کرتی ہے۔ یہ اینڈرائیڈ
) آئی او ایس دونوں کے لیے دستیاب ہے۔ بالترتیب
100) کی مؤثر رینج کے ساتھ **m – 60m**۔

Briar
ایک میسجنگ ایپ ہے جو کارکنوں، صحافیوں، اور کسی بھی ایسے شخص کے لیے بنائی گئی ہے جسے بات چیت کے لیے محفوظ اور آسان طریقے کی ضرورت ہے۔ یہ بلوٹوتھ یا وائی فائی کا استعمال کرتا ہے تاکہ کسی بحران میں معلومات کی روانی برقرار رہے۔ یہ صرف اینڈرائیڈ پر دستیاب ہے۔

Bridgefy
ایک میسجنگ ایپ ہے جو صارفین کو ایڈہاک نیٹ ورکس جیسے پیئر۔ٹو۔پیئر وائی فائی اور بلوٹوتھ کے ذریعے خفیہ کردہ پیغامات بھیجنے کی اجازت دیتی ہے۔ یہ اینڈرائیڈ اور آئی او ایس دونوں کے لیے دستیاب ہے۔

نوٹ: ان ایپس کو تخفیف کی حکمت عملی کے طور پر تجویز کیا گیا ہے نہ کہ پیغامات کی غیر قانونی مداخلت کے حل طور پر یا مکمل طور پرجوابی اقدام کے طور پر۔

پاکستان میں نگرانی کی صلاحیتوں کے بارے میں ہم اب تک کیا جانتے ہیں:

۱)
کو یقینی **"** پنجاب سیف سیٹیز اتھارٹی کو احتساب کے واسطے اور جرائم میں کمی کے لیے ''عوامی مقامات کی بہتر نگرانی[3] کے تحت رکھا جاتا ہے۔ تاہم اس بنانے کا اختیار حاصل ہے۔ جمع کیے گئے ڈیٹا کو ''ڈیٹا اور پرائیویسی پروٹیکشن پروسیجرز[4] کار میں **(DP3)**

[3] Berhan Taye, "Pakistan shuts down the internet three times in one week," Access Now, November 6, 2018, https://www.accessnow.org/pakistan-shutdowns-internet/.
[4] https://psca.gop.pk/wp-content/uploads/2021/03/PrivacyPolicyDP3.pdf

نفاذ کے حوالے سے شفافیت کا فقدان ہے، اور شہریوں کے ڈیٹا کی ریکارڈنگ اور پروسیسنگ شہری آزادیوں کے لیے "
۔تشویش کا باعث ہے

۲)

2019 کہ پاکستانی حکومت نے پاکستان ٹیلی کمیونیکیشن اتھارٹی میں یہ اطلاع ملی[5]
2010 (PTA)، کی جانب سے ٹیلی فونی ٹریفک ریگولیشنز
کے مینڈیٹ کے تحت ڈیپ پیکٹ انسپیکشن کا استعمال کرتے ہوئے پاکستان میں انٹرنیٹ ٹریفک کی نگرانی کے لیے کینیڈا
۔کی کمپنی سینڈ وائن کی خدمات حاصل کرنے کا عہد کر دیا ہے[6]
اگرچہ اس بات کی تصدیق کی گئی تھی کہ پاکستانی حکومت نے سینڈ وائن کے ساتھ معاہدہ کیا تھا لیکن یہ سارا لین دین
۔شفافیت کے فقدان کا شکار ہو چکا ہے

۳)

دی سیٹیزن لیب کے ذریعے کی گئی کمپیوٹر فوریننزک تحقیق کے مطابق
Finfisher انٹریوژن
۔میلویئر سویٹ، پاکستان میں آپریشنل پایا گیا ہے[7]

۴)

CitizenLab
جس میں انہوں نے میں ایک رپورٹ شائع کی[8]
2019
NSO کے **Pegasus** کے
اسپائی ویئر کو 45 ممالک میں آپریشنل پایا، جہاں پاکستان بھی اس فہرست کا حصہ تھا۔ اس بارے میں مزید کوئی قابل
۔۔تصدیق معلومات نہیں مل سکیں

: مواصلات کی نگرانی پاکستان میں متعدد قوانین کے ذریعے منظم ہے

- انویسٹی گیشن فار فیئر ٹرائل ایکٹ (2013) بنیادی طور پر کسی بھی مجاز افسر
(BPS-20)
اور اس سے اوپر کے ذریعے آلات کو روکنے اور ٹریک کرنے کے لیے ٹیکنالوجی کے استعمال کو ہائی کورٹ کے جج کے ذریعے
نگرانی کے لیے وارنٹ جاری کرنے پر قانونی حیثیت دیتا ہے تاکہ کامیابی کے ساتھ جرائم کو روکنے کے اقدامات انجام دیئے جا
۔سکیں۔ اور ایکٹ کے دیباچے کے مطابق قانون نافذ کرنے والے اداروں کے لیے ایک ناگزیر امداد بنیں

---

[5] https://www.codastory.com/authoritarian-tech/surveillance/pakistan-nationwide-web-monitoring/
[6] https://www.dawn.com/news/1484245
[7] https://citizenlab.ca/2015/03/finfisher-lawsuit-to-be-heard-in-pakistans-lahore-high-court/
[8] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

- پریوینشن آف الیکٹرانک کرائمز ایکٹ (2016) میں ٹریفک ڈیٹا کی توسیعی برقراری، ہتک عزت کی مجرمانہ کارروائی، اور پی ٹی اے
PTA
کے ذریعے آن لائن مواد پر مجموعی طور پر کنٹرول کے حصے شامل ہیں۔

- **S .4**
کے ذریعے ٹیلی فونی ٹریفک ریگولیشنز (2010) کی نگرانی اور مفاہمت کے لیے ہر طویل فاصلے اور بین الاقوامی سروس فراہم کرنے والے کو ایک ایسا نظام قائم کرنے کی ضرورت ہے جو پی ٹی اے کے نیٹ ورکس پر ٹریفک کی ریئل ٹائم نگرانی اور ریکارڈنگ کی اجازت دیتا ہے۔

- پاکستان ٹیلی کمیونیکیشنز (ری آرگنائزیشن) ایکٹ، 1996 قومی سلامتی کے مفاد میں کالز اور پیغامات کو روکنے کی اجازت دیتا ہے۔
54(1) سیکشن

آپ کے آلات کی نگرانی کے بارے میں ایک گائیڈ:

احتجاج کے دوران موبائل فون کیسے استعمال کیا جا سکتا ہے اور ڈیٹا کے ارد گرد خطرات کو کیسے کم کیا جائے۔

موبائل فون ڈیٹا نکالنے کے اوزار کیا کرتے ہیں؟
موبائل فون ڈیٹا نکالنے (موبائل فون ایکسٹریکشن یعنی ایم پی ای) ٹولز ایسے آلات ہیں جو پولیس کو موبائل فون سے ڈیٹا نکالنے کی اجازت دیتے ہیں۔ بشمول

۱) رابطے
۲) کال ڈیٹا (یعنی آپ کس کو کال کرتے ہیں، کب، اور کتنی دیر تک)
۳) ٹیکسٹ پیغامات (بشمول آپ نے کس کو اور کب ٹیکسٹ کیا)
۴) ذخیرہ شدہ فائلیں (تصاویر، ویڈیوز، آڈیو فائلیں، دستاویزات) وغیرہ
۵) ایپ ڈیٹا (ان ایپس پر محفوظ کردہ ڈیٹا) سمیت
۶) مقام کی معلومات اور تاریخ
۷) وائی فائی نیٹ ورک کنکشنز (جو کسی بھی ایسی جگہ کے مقامات کو ظاہر کر سکتے ہیں جہاں آپ نے وائی فائی منسلک کیا ہے، جیسے آپ کے کام کی جگہ یا کیفے)۔
۸) ایم پی ای ٹولز کلاؤڈ میں محفوظ کردہ ڈیٹا تک بھی رسائی حاصل کر سکتے ہیں لہذا یہاں تک کہ اگر آپ اپنے جمع شدہ ڈیٹا کو کم سے کم کرنے کے بارے میں بہت محتاط ہیں، تب بھی اس تک رسائی حاصل کی جا سکتی ہے اگر یہ آن لائن محفوظ ہے۔ یا وہ ڈیٹا جو آپ کو معلوم بھی نہیں ہے اور یہاں تک کہ وہ ڈیٹا جس کو حذف کر دیا گیا ہے، اس تک بھی رسائی ممکن ہے۔

احتجاج میں موبائل فون ڈیٹا نکالنے کے آلات کیسے استعمال کیے جا سکتے ہیں؟

محفوظ شدہ ڈیٹا کو نکالنے کے لیے، پولیس کو جسمانی طور پر آپ کے موبائل فون تک رسائی کی ضرورت ہوگی۔ پولیس آپ کا فون لے سکتی ہے اگر آپ کو کسی احتجاج کے دوران حراست میں لیا گیا یا گرفتار کیا گیا یا تلاشی لی گئی، لیکن تب بھی کہ اگر آپ گواہ ہیں یا آپ کسی جرم کا شکار بھی ہوئے ہیں تو۔

احتجاج پر جاتے وقت کیا سوچنا چاہیے۔

اپنے فون کے آپریٹنگ سسٹم
(iOS یا Android)
کو اپ ٹو ڈیٹ رکھنا ہے جس کا مطلب ہے کہ اس میں تازہ ترین سیکیورٹی خصوصیات ہوں ،یہ ایم پی ای کو روکنے کا بہترین طریقہ ہے۔

اگرچہ ایم پی ای سے اپنے آپ کو بچانے کا سب سے مؤثر طریقہ یہ ہے کہ آپ اپنے فون کو احتجاج میں نہ لے کر جائیں، لیکن یہ ایک حقیقت پسندانہ حل ہونے کا امکان نہیں رکھتا ہے۔ درحقیقت، آپ کا فون نہ ہونا آپ کو دوسرے طریقوں سے کمزور بنا سکتا ہے۔ اگر آپ کے پاس کم سے کم ڈیٹا والا متبادل فون ہے تو اسے لے جانا بہتر ہوگا۔

اگرچیکه آپ کو اپنے فون کو مقفل رکھنا چاہیے، کچھ ایم پی ای ٹولز کو مبینہ طور پر لاک فون تک رسائی کے لیے ڈیزائن کیا گیا ہے۔ تاہم، اس سیکیورٹی کو نظرانداز کرنے کی ان کی صلاحیت فون اور اس کے آپریٹنگ سسٹم پر منحصر ہے۔

احتجاج میں جانے سے پہلے، آپ اپنے فون کے ڈیٹا کو اپنے کمپیوٹر میں بیک اپ کرنے، اور پھر اس ڈیٹا کو اپنے فون سے ہٹانے پر غور کر سکتے ہیں۔ لیکن آپ کو معلوم ہونا چاہئے کہ کچھ ایم پی ای ٹولز حذف شدہ ڈیٹا کو بازیافت کرنے کے قابل ہیں۔ اگر آپ نے ڈیٹا کو کلاؤڈ سروس میں محفوظ کر لیا ہے، تو کچھ ایم پی ای ٹولز تب بھی اس ڈیٹا تک رسائی حاصل کر سکتے ہیں۔

۔کلاؤڈ ایکسٹریکشن ٹولز کو احتجاج میں کیسے استعمال کیا جا سکتا ہے اور آپ اپنےڈیٹا کے پھیلاؤ کو کیسے کم سے کم کر سکتے ہیں:

؟کلاؤڈ ڈیٹا نکالنے کے اوزار کیا ہیں اور وہ کیا کرتے ہیں

کلاؤڈ ڈیٹا نکالنے کی ٹیکنالوجی پولیس کو آپ کے موبائل فون یا دیگر آلات کے ذریعے آپ کے 'کلاؤڈ' میں محفوظ کردہ ڈیٹا تک رسائی کے قابل بناتی ہے۔

کلاؤڈ سے ڈیٹا نکالنے والے ٹولز کے استعمال کا مطلب ہے کہ پولیس اس ڈیٹا تک رسائی حاصل کر سکتی ہے جسے آپ آن لائن اسٹور کرتے ہیں۔ کلاؤڈ میں ڈیٹا اسٹور کرنے والی ایپس میں
Uber , Slack, Instagram, Telegram, Twitter, Facebook
کی مثالیں موجود ہیں ۔

؟احتجاج میں کلاؤڈ ڈیٹا نکالنے کے اوزار کیسے استعمال کیے جا سکتے ہیں

آپ کا کلاؤڈ ڈیٹا نکالنے کے لیے پولیس کو جسمانی طور پر آپ کے موبائل فون تک رسائی کی ضرورت ہوگی۔ پولیس آپ کا فون ضبط کر سکتی ہے اگر آپ کو احتجاج کے دوران حراست میں لیا گیا یا گرفتار کیا گیا ہے لیکن یہ رسائی تب بھی ممکن ہے اگر آپ نے کسی قسم کا جرم کیا ہے اور یہاں تک کہ اگر آپ کسی جرم کا شکار ہوئے ہیں ۔(موبائل فون نکالنے کے بارے میں احتجاجی گائیڈ بھی دیکھیں)۔
یہ تمام معلومات مظاہرین اور منتظمین کی شناخت ، احتجاج اور کارروائیوں کے مقامات کے بارے میں معلومات جاننے کے لیے استعمال کی جا سکتی ہیں۔
آپ کا کلاؤڈ ڈیٹا صرف آپ کے بارے میں معلومات کو ظاہر نہیں کرتا ہے بلکہ یہ آپ کے دوستوں، خاندان، اور کسی بھی عزیز کے بارے میں بھی بہت کچھ ظاہر کر سکتا ہے جن سے آپ آن لائن بات چیت کرتے ہیں، جیسے کہ ساتھی مظاہرین، مثال کے طور پر آپ کے کلاؤڈ میں پرانے رابطے محفوظ ہو سکتے ہیں جنہیں فون سے ہی حذف کر دیا گیا ہو۔

؟احتجاج پر جاتے وقت کیا سوچنا چاہیے

آپ اپنے فون کو گھر پر چھوڑنے پر غور کر سکتے ہیں، اگر یہ حقیقت پسندانہ حل نہیں ہے تو آپ اپنے فون پر جو ایپلیکیشنزاستعمال کرتے ہیں ان میں کلاؤڈ بیک اپ کو بند کرنے اور تمام کلاؤڈ بیسڈ سروسز سے لاگ آؤٹ کرنے کے بارے میں سوچنا چاہیے۔ یہ کلاؤڈ میں ڈیٹا کو محفوظ ہونے سے بچائے گا اور آپ کے موبائل فون سے اس ڈیٹا تک کی رسائی کو روک دے گا۔

کسی احتجاج میں جانے سے پہلے، آپ کو اس بات سے آگاہ ہونا چاہیے کہ اگرچہ آپ واٹس ایپ کے ذریعے اینڈ ٹو اینڈ انکرپٹڈ میسجنگ استعمال کرتے ہیں، اگر آپ واٹس ایپ پیغامات کا کلاؤڈ پر بیک اپ لیتے ہیں تو پولیس کلاؤڈ نکالنے والے ٹولز کے ذریعے ان انکرپٹڈ بیک اپس تک رسائی حاصل کر سکتی ہے۔

آپ کلاؤڈ میں کچھ ایپلیکیشنز، جیسے واٹس ایپ ، فیس بک،اوبر اور ٹویٹر میں

محفوظ ہونے والے مقاماتی ڈیٹا کی رسائی کو بند کر سکتے ہیں۔ اس سے پولیس کو یہ معلوم کرنے سے روکا جا سکتا ہے کہ آپ کہاں کہاں گئے تھے۔

IMSI

کیچرز کو احتجاج میں کیسے استعمال کیا جا سکتا ہے اور آپ اپنے ڈیٹا کو لاحق خطرات کو کیسے کم کر سکتے ہیں

2015

پنجاب پولیس کے کاؤنٹر ٹیررازم ڈیپارٹمنٹس میں تعیناتی کے لیے میں پنجاب انفارمیشن ٹیکنالوجی بورڈ نے[9]
آئی ایم ایس آئی کیچرز کی خریداری کے لیے ایک ٹینڈر نوٹس جاری کیا۔

IMSI کیچر کیا ہے؟

آئی ایم ایس آئی کا مطلب بین الاقوامی موبائل سبسکرائبر شناخت ہے جو آپ کے سم کارڈ کے بنیاد پر بنایا جانے والا ایک منفرد نمبر ہے۔ آئی ایم ایس آئی کیچر کو
Stingrays کے نام سے بھی جانا جاتا ہے۔

IMSI، کیچر ایک ایسا آلہ ہے جو اپنے آپ کو ایک موبائل سیل ٹاور کے طور پر ظاہر کرتا ہے اور آس پاس کے تمام موبائل فونز کے منفرد آئی ایم ایس آئی نمبر کو کیچ کر کے ان کے کو ٹریک کرنے کے لیے ان سے جڑنے کی کوشش کرتا ہے۔

یہ زبردست سگنل کی طاقت کے ساتھ موبائل فون ٹاور ہونے کا بہانہ کر کے، قریبی موبائل فونز کو اپنے سے جوڑنے کے لیے دھوکہ دے کر اس طرح سے جڑ جاتا ہے کہ فون صارف کے علم کے بغیر اس فون سے ڈیٹا کو نچوڑ سکے۔

اس صورتحال میں آپ کے بارے میں سب سے زیادہ قابل رسائی معلومات آپ کا مقام ہے۔ یہ ناگزیر ہے کہ سیل ٹاورز آپ کے محل وقوع کو مثلث کے ذریعے جانتے ہیں, درحقیقت اس طرح وہ آپ کو پہلے اپنی سروس فراہم کرتے ہیں۔ خود کو آپ اور سیل ٹاور کے درمیان رکھ کر ایک آئی ایم ایس آئی کیچر آپ کی لوکیشن کا تعین کر سکتا۔

آئی ایم ایس آئی کیچرز فون پر ذخیرہ شدہ ڈیٹا کو نہیں پڑھتے ہیں۔ اس کے بجائے، ان آلات کے ٹیکسٹ پیغامات اور فون کالز کو روکنے کی کوشش کرنے کے لیے استعمال کیا جا سکتا ہے۔

آئی ایم ایس آئی کیچر کی صلاحیتوں اور آپ کا فون جس نیٹ ورک سے منسلک ہو رہا ہے اس پر منحصر ہے کہ مزید جدید حملے ہو سکتے ہیں یا نہیں اگرچہ اس کا امکان نہیں ہے۔ کچھ
Stingray

[9] https://eproc.punjab.gov.pk/BiddingDocuments/35144_Tender%20Doc%20-%20Security%20Items%20for%20CTD%20Police%20Stations%20-%20105052015-1.pdf

آلات کمیونیکیشن پروٹوکولز کی جان کردہ کمزوریوں پر انحصار کرتے ہیں اور آپ کے فون کو اپنے استعمال کردہ پروٹوکولز کو ڈاؤن گریڈ کرنے پر مجبور کر سکتے ہیں، تاکہ آپ کی کمیونیکیشنز کو کم محفوظ اور زیادہ آسانی سے قابل رسائی بنایا جا سکے (مثلا **G2,G 3**
پر رابطے کو کم کر کے -

آئی ایم ایس آئی پکڑنے والے ان انکرپٹڈ پیغامات کے مواد کو نہیں پڑھ سکتے جن کا آپ پلیٹ فارمز کے ذریعے تبادلہ کرتے ہیں (جیسے سگنل، واٹس ایپ، وائر جو اینڈ ٹو اینڈ انکرپشن استعمال کرتے ہیں (جیسے سگنل، واٹس ایپ، وائر)-

IMSI(؟آئی ایم ایس آئی) کیچرز کو احتجاج میں کیسے استعمال کیا جا سکتا ہے

پولیس آئی ایم ایس آئی کیچرز کا استعمال اس بات کی نشاندہی کرنے کے لیے کر سکتی ہے کہ احتجاج میں کون کون شامل تھا، ان تمام فونز کے آئی ایم ایس آئی نمبرز حاصل کر کے جو اس احتجاج میں آپس میں آس پاس موجود تھے-

آئی ایم ایس آئی کیچرز کی کچھ قسمیں پولیس کو اس قابل بھی بنا سکتی ہیں کہ وہ احتجاج کو روکیں یا ہونے سے پہلے ہی روک سکیں-

مثال کے طور پران کا استعمال آپ کی کالز اور پیغامات کی نگرانی یا ان کو بلاک کرنے کے لیے کیا جا سکتا ہے۔ آپ کے علم کے بغیر اپ کے پیغامات میں ترمیم کر سکیں یا یہاں تک کہ آپ ہی ہونے کا بہانہ کرتے ہوئے کسی کو پیغام لکھیں اور بھیجیں-

احتجاج پر جاتے وقت کیا سوچنا ہے-

اپنے فون کو ایئروپلین موڈ میں رکھنے یا اسے مکمل طور پر بند کرنے کا مطلب یہ ہوگا کہ آئی ایم ایس آئی کیچر آپ کو یا آپ کے مواصلات کو ٹریک نہیں کر سکتا -

آپ اپنے ٹیکسٹ پیغامات کے مواد کو آئی ایم ایس آئی کیچر کے ذریعے ٹریک کیے جانے سے روکنا چاہتے ہیں تو آپ ایسی پیغام رسانی ایپس کی خدمات استعمال کر سکتے ہیں جو اینڈ ٹو اینڈ انکرپشن استعمال کرتی ہیں، جیسے سگنل، واٹس ایپ اور فیس بک، آئی ایم ایس آئی ممکنہ طور پر صرف وہ معلومات اکٹھا کر سکتا ہے کہ آپ یہ میسجنگ ایپس استعمال کر رہے ہیں، نہ کہ خود اس کے ذریعے بھیجا گیا مواد کیا ہے-

حلانکہ آئی ایم ایس آئی کیچرز فون پرجمع شدہ ڈیٹا کو نہیں پڑھتے ہیں، اس بات کو ذہن میں رکھیں کہ پولیس کے پاس دوسری ٹیکنالوجی بھی ہوسکتی ہے جو انہیں آپ کے فون پر ڈیٹا تک رسائی کے قابل بنا سکتی ہے، جیسے کہ موبائل فون ڈیٹا ایکسٹریکشن اورہیکنگ ٹولز-

سوشل میڈیا مانیٹرنگ کو احتجاج میں کیسے استعمال کیا جا سکتا ہے اور آپ اپنے ڈیٹا کے خطرات کو کیسے کم کر سکتے ہیں۔

سوشل میڈیا مانیٹرنگ کیا ہے؟

سوشل میڈیا مانیٹرنگ سے مراد سوشل میڈیا پلیٹ فارمز، جیسے فیس بک، ٹویٹر، انسٹاگرام اور ریڈٹ پر شیئر کی گئی معلومات کی نگرانی، اسے جمع کرنا اور اس کا تجزیہ کرنا ہے۔

اس میں پبلک یا پرائیویٹ گروپس یا پیجز پر پوسٹ کیے گئے مواد کی جاسوسی بھی شامل ہو سکتی ہے۔ اس میں "اسکریپنگ" بھی شامل ہو سکتی ہے - سوشل میڈیا پلیٹ فارم سے تمام ڈیٹا کو جمع کرنا، بشمول آپ جو مواد پوسٹ کرتے ہیں اور آپ کے رویے کے بارے میں ڈیٹا (جیسے کہ آپ کیا پسند کرتے ہیں اور شیئر کرتے ہیں)۔

اسکریپنگ اور دیگر ٹولز کے ذریعے، سوشل میڈیا مانیٹرنگ سوشل میڈیا ڈیٹا کے ایک وصیح ذخیرے کو جمع کرنے اور تجزیہ کرنے کی اجازت دیتی ہے جسے صارفین کے بارے میں پروفائلز اور پیشین گوئیاں بنانے کے لیے استعمال کیا جا سکتا ہے۔

سوشل میڈیا مانیٹرنگ کو احتجاج کے سلسلے میں کس طرح استعمال کیا جاتا ہے؟

احتجاج کے منتظمین اکثر احتجاج کو منظم کرنے، مظاہرین کے ساتھ بات چیت کرنے، اور احتجاج کی تصاویر اور ویڈیوز اپ لوڈ کرنے کے لیے سوشل میڈیا کا استعمال کریں گے۔

بدلے میں اس کا مطلب ہے کہ پولیس سوشل میڈیا کے صفحات اور گروپس کو 'ڈیٹا مائن' کر سکتی ہے تاکہ منتظمین کی شناخت اور وابستگیوں، منصوبہ بندی کی کارروائی کا مقام اور وقت اور دیگر متعلقہ معلومات جاننے کی کوشش کی جا سکے۔

پولیس مظاہرین کی شناخت کے لیے ماضی یا مستقبل کے احتجاج سے متعلق سوشل میڈیا پوسٹس کو ٹریک کر سکتی ہے۔

پولیس مظاہرین کی شناخت کے لیے سوشل میڈیا پر اپ لوڈ کی جانے والی احتجاجی تصاویر اور ویڈیوز کے لیے چہرے کی شناخت کی ٹیکنالوجی یا گیٹ ریکگنیشن ٹیکنالوجی کا بھی استعمال کر سکتی ہے۔

احتجاج پر جاتے وقت کیا سوچنا چاہیے؟

اگر آپ اپنی احتجاجی تصاویر اپنے سوشل میڈیا اکاؤنٹس پر اپ لوڈ کرتے ہیں تو ان کا استعمال کسی احتجاج کے مقام پر افراد کی شناخت کرنے اور انہیں رکھنے کے لیے کیا جا سکتا ہے۔
اگر آپ کے مقام کی سیٹنگ آپ کے سوشل میڈیا پلیٹ فارمز یا آپ کے کیمرہ اور فوٹو ایپس کے لیے آن ہیں اور پھر آپ احتجاج کی جگہ سے یا اس کے قریب سے آن لائن پوسٹ کرتے ہیں، تو پولیس اس مقام کے ڈیٹا تک رسائی حاصل کر سکتی ہے۔

اگر آپ احتجاج کے دوران سوشل میڈیا استعمال کرنا چاہتے ہیں تو آپ کو اس پلیٹ فارم پر اپنے مقامی یعنی لوکیشن کی سیٹنگ کو بند کرنے پر غور کرنا چاہیے جسے آپ استعمال کریں گے۔ اگر آپ احتجاجی تصاویر شیئر کرنے کا فیصلہ کرتے ہیں تو ایسے افراد کو ٹیگ نہ کریں جن کی رضامندی یا کنسینٹ نہیں لی گئی کیونکہ یہ ایک ایسا ذریعہ بن سکتا ہے جس سے پولیس لوگوں کو شناخت کر سکتی ہے۔

EXIF ۔اگر آپ سوشل میڈیا اکاؤنٹس پر اپنی احتجاجی تصاویر اپ لوڈ کرنا چاہتے ہیں تو پہلے ڈیٹا کو ہٹانے پر غور کریں ڈیٹا آپ کی تصاویر سے وابستہ میٹا ڈیٹا ہے **EXIF**

۔جو کافی معلومات کو ظاہر کر سکتا ہے جیسے کہ مقام، وقت اور تاریخ اور استعمال شدہ ڈیوائس

ہوشیار رہیں، فوٹیج کی لوکیشن سیٹنگز آف کرنے کے بعد بھی پس منظر میں موجود معلومات سے جغرافیائی محل وقوع کی شناخت کی جا سکتی ہے (مثلاً کوئی یادگار یا تاریخی نشان)۔ اپنے اردگرد کی فلم بناتے وقت اسے ذہن میں رکھیں اور قابل شناخت پس منظر سے بچنے کی کوشش کریں۔

اگر ممکن ہو تو، تصویریں اور ویڈیوز صرف تب اپ لوڈ کریں جب آپ اس جگہ سے باہر نکل جائیں تاکہ ٹریک یا فالو کیے جانے سے بچایا جا سکے اور کسی بھی بصری ڈیٹا کو اپ لوڈ کرتے وقت
VPN
استعمال کریں۔

ہیکنگ کو احتجاج میں کیسے استعمال کیا جا سکتا ہے اور آپ اپنے ڈیٹا کے ارد گرد خطرات کو کیسے کم کر سکتے ہیں۔

؟ہیکنگ کیا ہے

ہیکنگ سے مراد سسٹمز میں موجود کمزوریوں کو تلاش کرنا ہے، یا تو ان کی اطلاع دینا اور ان کی مرمت کرنا، یا ان کا استحصال کرنا۔

ہیکنگ سے ان آلات، نیٹ ورکس اور خدمات میں حفاظتی خامیوں کی نشاندہی کرنے میں مدد مل سکتی ہے جنہیں لاکھوں لوگ استعمال کرتے ہیں اور جب سسٹم ڈیزائنرز کو اطلاع دی جاتی ہے تو عام طور پر ٹھیک کر دی جاتی ہے۔ لیکن ہیکنگ کا استعمال ہمارے آلات تک رسائی کے لیے بھی کیا جا سکتا ہے تاکہ خفیہ طور پر ہمارے بارے میں معلومات اکٹھی کی جا سکیں اور ممکنہ طور پر ہمیں اور ہمارے آلات کی دوسرے طریقوں سے ہیرا پھیری کر سکیں۔

ہیکنگ کا عمل ہمیشہ سے ابھرتی ہوئی تکنیکوں پر مشتمل ہے۔ یہ دور سے بیٹھے بھی کیا جا سکتا ہے لیکن اس میں کسی ڈیوائس یا سسٹم کے ساتھ جسمانی مداخلت بھی شامل ہو سکتی ہے ۔ مثال کے طور پر موبائل فون کو ان لاک کرنے پر مجبور کرنا۔

اس میں لوگوں کی ٹیکنالوجی تک رسائی حاصل کرنے کے لیے ان سے فائدہ اٹھانا بھی شامل ہو سکتا ہے۔ ایک مثال 'فشنگ' کی ہوگی، جہاں ایک حملہ آور مالویئر سے متاثرہ لنک یا منسلکہ فائل بھیجنے کے لیے کسی قابل اعتماد شخص یا تنظیم کی نقالی کرتا ہے۔

میں پیگاسس جیسے ہیکنگ میلویئر کے پاکستان اور 44 دیگر ممالک میں استعمال سیٹیزن لیب کی 2019 کی رپورٹ[10] ہونے کی اطلاع دی گئی ہے۔
Pegasus
ٹیکنالوجی ممکنہ طور پر
iOS اور **Android**
آلات کی ایک بڑی تعداد کو متاثر کرنے کے لیے استعمال کی جا سکتی ہے۔

ہیکنگ کو احتجاج میں کیسے استعمال کیا جا سکتا ہے؟

پولیس، مثال کے طور پر آئی ایم ایس آئی کیچرز کے استعمال کے ذریعے مواصلات کو ہیک کرنے کے قابل ہے۔ کیچرز صرف اس معلومات تک رسائی حاصل کر سکتے ہیں جو موبائل ڈیوائس اور سیل ٹاور کے درمیان منتقل ہو رہی ہے۔آئی ایم ایس آئی کیچرز اس معلومات تک رسائی حاصل نہیں کر سکتے جو آلے پر محفوظ کی گئی ہے۔

اس لیے پولیس فون، لیپ ٹاپ یا دیگر انٹرنیٹ سے منسلک ڈیوائس پر ذخیرہ شدہ معلومات تک ریموٹ رسائی حاصل کرنے کے لیے جدید ترین ہیکنگ تکنیکوں کا استعمال کر سکتی ہے جو مظاہروں کو منظم کرنے یا اس میں حصہ لینے کے لیے استعمال ہوتی ہے۔ چاہے وہ پاس ورڈ، فنگر پرنٹ یا فیس انلاک کی تکنیک سے محفوظ ہوں۔

پولیس کسی بھی ایسے آلات کو اکٹھا کر سکتی ہے اور ان تک رسائی حاصل کر سکتی ہے جو احتجاج میں مظاہرین سے گرائے، کھوئے یا ضبط کیے جائیں۔

احتجاج پر جاتے وقت کیا سوچنا ہے۔

اپنے آلے کو اپ ٹو ڈیٹ رکھنا ہیکنگ کو روکنے کا ایک اچھا طریقہ ہے کیونکہ ہیکنگ اکثر ان کمزوریوں کا فائدہ اٹھاتی ہے جن کا انکشاف تو ہو چکا ہے لیکن ابھی تک پیچ نہیں کیا گیا ہے۔
یقینی بنائیں کہ آپ کا آلہ اپنے آپریٹنگ سسٹم
(Android یا **iOS)**
کا تازہ ترین دستیاب ورژن چلا رہا ہے اور آپ کی سیکیورٹی کو بہتر بنانے اور ہیکنگ کے خطرے کو کم کرنے کے لیے آپ کی تمام ایپس اپ ٹو ڈیٹ ہیں۔

[10] https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

آپ کو اپنے فون یا دیگر الیکٹرانک آلات کو مقفل رکھنا چاہیے، کچھ ہیکنگ تکنیکیں مقفل آلات تک بھی رسائی حاصل کر سکتی ہیں۔ اس سیکیورٹی کو نظرانداز کرنے کی ان کی اہلیت موجود ہے، تاہم اس کا انحصار ہیکنگ کی تکنیک اور اس کے ہدفیہ آلے پر ہے۔

کسی احتجاج میں جانے سے پہلے، اگر ممکن ہو تو آپ اپنے فون کے ڈیٹا کا بیک اپ کسی دوسرے آلے پر منتقل کر دیں۔ لیکن آپ کو معلوم ہونا چاہیے کہ کچھ ہیکنگ ٹولز حذف شدہ ڈیٹا کو بازیافت کرنے کے قابل ہوتے ہیں۔ اگر آپ نے ڈیٹا کو کلاؤڈ سروس میں محفوظ کر لیا ہے، تو کچھ ہیکنگ ٹولز اب بھی اس ڈیٹا تک رسائی حاصل کر سکتے ہیں۔

فریب دہی حملوں سے بچنے کے لیے آپ کو ہمیشہ اس بارے میں محتاط رہنا چاہیے کہ آپ کن لنکس پر کلک کرتے ہیں۔

آپ کے چہرے اور جسم کی نگرانی سے بچاؤ کے لیے ایک گائیڈ

چہرے کی شناخت کی تکنیک کو احتجاج میں کیسے استعمال کیا جا سکتا ہے اور آپ اپنی پہچان کو ظاہر نہ کرنے کی کوشش کیسے کر سکتے ہیں

چہرے کی شناخت کی ٹیکنالوجی کیا ہے؟
چہرے کی شناخت کی ٹیکنالوجی (ایف آر ٹی)
لوگوں کے چہروں کے بارے میں ڈیٹا اکٹھا کرتی ہے اور اس پر کارروائی کرتی ہے
اور یہ لوگوں کی شناخت کے لیے استعمال کی جا سکتی ہے۔

ایف آر ٹی کی گئی تصاویر کو موجودہ ڈیٹا بیس یا واچ لسٹ میں محفوظ کردہ تصاویر کے ساتھ ملاتا ہے۔ پاکستان کسٹمز ڈپارٹمنٹ کی جانب سے چہرے کی شناخت کی ٹیکنالوجی پر انحصار کرتے ہوئے ایک نیشنل ٹارگٹنگ سینٹر (این ٹی سی) قائم کرنے کی اطلاع[11] دی گئی تھی جو امیگریشن ڈیپارٹمنٹ، نادرا، ایڈوانس پیسنجر انفارمیشن سسٹم، نیشنل کسٹمز انفورسمنٹ نیٹ ورک سمیت متعدد سرکاری اداروں کے ساتھ منسلک ہوگا۔ یہ نظام پاکستان کسٹمز اور قانون نافذ کرنے والے اداروں کو ممکنہ طور پر خطرناک افراد اور نقل و حمل کی پروفائلنگ میں مدد کرنے کی آڑ میں بنایا گیا ہے۔

احتجاج پر جاتے وقت کیا سوچنا چاہیے؟

[11] https://www.dawn.com/news/1584264

اگر آپ اپنا نام یا پہچان ظاہر نہ کرنے کی کوشش کرنا چاہتے ہیں تو آپ چہرے کو ڈھانپنے کی تجاویز پر غور کریں، جیسے ماسک پہننا، جو ایف آر ٹی
۔کے لیے آپ کے چہرے کے خدوخال کی درست تصاویر کھینچنا مشکل بنا سکتا ہے
ایف آر ٹی میں خلل ڈالنے کے دیگر اختیارات میں چہرے کی پینٹ اور ایسے ڈیزائنوں کے ساتھ کپڑوں کا استعمال شامل ہے
FRT ، جن کا مقصد چہرے کی درست شناخت میں مداخلت کرنا ہے۔ تاہم اس تکنیک میں
مسلسل تبدیلیاں آ رہی ہیں اور بدلاؤ ہو رہا ہے، اس لیے چہرے کو ڈھانپنا اور اس طرح کے دوسرے طریقے مستقبل میں
۔کم موثر ثابت ہو سکتے ہیں
۔پولیس کے اختیارات ثقافتی تناظر اور دائرہ اختیار کے لحاظ سے مختلف ہوتے ہیں

کا استعمال کر سکتی ہے، اس لیے کسی **FRT** چونکہ پولیس سوشل میڈیا پر تصاویر یا ویڈیو ریکارڈنگز کا تجزیہ کرنے کے لیے
۔احتجاج کی کوئی بھی تصویر پوسٹ کرنے سے پہلے اس پر غور کریں جس میں دوسرے مظاہرین کے چہرے نمایاں ہوں

اس طرح، آپ آن لائن تصاویر یا ویڈیوز پوسٹ کرنے سے پہلے چہرے کو دھندلا کرنے والے ٹولز استعمال کرنے پر غور کر
۔سکتے ہیں

پولیس ڈرون ٹیکنالوجی کو احتجاج میں کیسے استعمال کیا جا سکتا ہے اور آپ اپنی شناخت ظاہر نہ کرنے کی کوشش کیسے
۔کر سکتے ہیں

عوامی اجتماعات کو محدود اور منظم کرنے اسلام آباد کیپٹل پولیس نے ستمبر 2022 میں امن و امان برقرار رکھنے کے لیے[12]
۔کے لیے غیر مہلک ڈرونز کی خریداری کا اعلان کیا تھا

؟پولیس ڈرون کیا ہیں

ڈرون مختلف سائز کی بغیر پائلٹ کے فضائی مشینیں ہیں جو عام طور پر کیمروں **(UAVs)** ۔کو دور سے کنٹرول کیا جاتا ہے
۔سے لیس ہوتے ہیں اور چہرے کی شناخت کی ٹیکنالوجی کے ساتھ بھی لیس ہو سکتے ہیں
ڈرونز سپیکر نگرانی کے آلات ریڈار اور کمیونیکیشن انٹرسیپشن ٹولز، جیسے
IMSI ۔کیچر آلات سے بھی لیس ہو سکتے ہیں

[12] https://tribune.com.pk/story/2375942/islamabad-police-to-use-non-lethal-drones-to-disperse-rioters

؟احتجاج کے دوران ڈرون کا استعمال کیسے ہو سکتا ہے

کیمرے سے لیس ڈرون کا استعمال عوامی مقامات پر لوگوں کی نقل و حرکت بشمول احتجاج کے دوران ان کی رضامندی کے بغیر یا ان کو آگاہ کیے بغیر بھی دور سے نگرانی کرنے کے لیے استعمال کیا جا سکتا ہے۔
اسی طرح جب کمیونیکیشن انٹرسیپشن ٹیکنالوجیز سے لیس ہو تو ڈرون کو مظاہرین کی کالز اور پیغامات کی نگرانی اور ٹریک کرنے کے لیے استعمال کیا جا سکتا ہے اس علاقے میں جہاں احتجاج ہو رہا ہو۔
اسپیکروں سے لیس ڈرونز کا استعمال مظاہرین کے ساتھ رابطہ کرنے کے لیے بھی استعمال کیا جا سکتا ہے مثال کے طور پر انہیں احکامات، ہدایات یا وارننگ دے کر۔

؟احتجاج پر جاتے وقت کیا سوچنا چاہیے

ڈرون کا استعمال اور آپ کی شناخت ظاہر نہ کرنے پر اثر ان ٹیکنالوجیز پر منحصر ہے جن سے وہ لیس ہیں۔

چہرے کی شناخت کرنے والی ٹیکنالوجی اور آئی ایم ایس آئی کیچرز کی گائیڈز پر غور کریں، کیونکہ یہ عام ٹولز ہیں جنہیں ڈرون مظاہرین کی سرگرمیوں کی نگرانی کے لیے استعمال کیا جا سکتا ہے۔

پولیسنگ ڈیٹا بیس اور پیشین گوئی کرنے والے پولیسنگ ٹولز کے حوالے سے ایک گائیڈ

Predictive Policing؟پریڈیکٹیو پولیسنگ) کیا ہے)

پولیس کی جانب سے پیشین گوئی کرنے والے پروگراموں کا استعمال اس بات کا اندازہ لگانے کے لیے کیا جاتا ہے کہ جرائم کہاں اور کب کیے جا سکتے ہیں یا ان کا ارتکاب کون کر سکتا ہے۔ یہ پروگرام کمپیوٹر الگورتھم کے ذریعے تاریخی پولیسنگ ڈیٹا کو استعمال کر کے کام کرتے ہیں۔
مثال کے طور پر ایک پروگرام ماضی کے جرائم کے بارے میں ڈیٹا کا جائزہ لے سکتا ہے تاکہ یہ اندازہ لگایا جا سکے کہ مستقبل میں جرائم کہاں ہوں گے - نقشے پر جرائم کے ہاٹ سپاٹ کی شناخت کرتا ہے لیکن یہ پروگرام جو ڈیٹا استعمال کرتے ہیں وہ نامکمل یا متعصب ہو سکتا ہے جس کی وجہ سے ''فیڈ بیک لوپ'' ہو سکتا ہے جس کی وجہ سے یہ پولیس اہلکاروں کا رخ ان کمیونٹیز کی طرف کر دیتا ہے جو پہلے سے ہی منفی طور پر زیادہ پولیسنگ کے رویہ کا شکار ہیں۔
دیگر پیش گوئی کرنے والے پولیسنگ پروگرام تجویز کر سکتے ہیں کہ لوگ کیسا برتاؤ کریں گے۔ ان پروگراموں میں کسی شخص کے بارے میں معلومات فراہم کی جاتی ہیں اور پھر وہ فیصلہ کرتے ہیں کہ آیا اس شخص کی طرف سے کوئی جرم کرنے کا امکان ہے۔

''وزارت انفارمیشن ٹیکنالوجی اور ٹیلی کمیونیکیشنز نے حال ہی میں ''کرائم

اینالیٹکس اینڈ سمارٹ پولیسنگ ان پاکستان کا آغاز کیا ہے جس کا مقصد پیشن گوئی کرنے والے پولیسنگ کے افعال کو انجام دینے کے لیے ڈیٹا اینالیٹکس کا استعمال کرنا ہے[13]۔ یہ پروگرام ملک بھر کے بڑے شہروں یعنی کراچی، اسلام آباد، گلگت، مظفرآباد اور کوئٹہ میں شروع کیا جائے گا[14]۔

پریڈیکٹیو پولیسنگ کو احتجاج میں کیسے استعمال کیا جا سکتا ہے؟

پولیس مظاہرین کی شناخت کرنے اور انہیں ڈیٹا بیس یا واچ لسٹ میں شامل کرنے کے لیے چہرے کی شناخت کرنے والی ٹیکنالوجی، آئی ایم ایس آئی کیچرز یا جیو لوکیشن ٹیکنالوجی کا استعمال کر سکتی ہے۔
کافی افراد اکثر اس بات سے بھی بے خبر ہوتے ہیں کہ آیا انہیں پولیس ڈیٹا بیس یا واچ لسٹ میں شامل کیا گیا ہے اور اس کے نتیجے میں ان کا اس سے ہٹانا اگر ناممکن نہیں تو بہت مشکل ہے۔

احتجاج پر جاتے وقت کیا سوچنا ہے۔

کوئی بھی تصویر، ویڈیوز یا پیغامات جو آپ کسی بھی آن لائن پلیٹ فارم پر احتجاج کے بارے میں شیئر کرتے ہیں ان کا تجزیہ پولیس مظاہرین کی شناخت کے لیے کر سکتی ہے۔ ایک بار شناخت ہونے کے بعد انہیں واچ لسٹ میں شامل کیا جا سکتا ہے یا ایسے پروفائلز بنانے کے لیے استعمال کیا جا سکتا ہے جو پھر پیش گوئی کرنے والے پولیسنگ ٹولز میں شامل ہو سکیں۔
اگر پولیس نے پہلے ہی آپ کو کسی ایسے شخص کے طور پر درجہ بندی کر رکھا ہے جس کس جرم کے ارتکاب کرنے کا امکان ہے، تو اس کا استعمال احتجاج کے دوران آپ کو حراست میں لینے، گرفتار کرنے یا روکنے اور تلاش کرنے کے لیے کیا جا سکتا ہے۔
عام طور پر حکومت کی طرف سے شفافیت کا فقدان اور حکومت کی کھلی پالیسیوں کی کمی ان ڈیٹا بیس کے غلط استعمال کے امکانات کو بڑھاتی ہے۔

قانون نافذ کرنے والے ڈیٹا بیس کو احتجاج میں کیسے استعمال کیا جا سکتا ہے۔

پنجاب سیف سٹیز اتھارٹی کے تحت پنجاب پولیس انٹیگریٹڈ کنٹرول اینڈ کمانڈ سنٹر

---

[13] "Changes underway for a unified, integrated policing system in country: Amin-ul-Haque", The Nation, August 20, 2022, https://www.nation.com.pk/20-Aug-2022/changes-underway-for-a-unified-integrated-policing-system-in-country-amin-ul-haque.
[14] Muhammad Saleh Zaafir, "Crime analytics and smart policing to be implemented in Pakistan: Aminul Haq," The News International, August 24, 2022, https://www.thenews.com.pk/print/984957-crime-analytics-and-smart-policing-to-be-implemented-in-pakistan-aminul-haq.

پی پی آئی سی 3)ایک ایسا ادارہ ہےجس کے پاس شہریوں کو فراہم کردہ سیکیورٹی کی سطح کو بڑھانے کے مقاصد کے لیے ڈیٹا اکٹھا کرنے کا مینڈیٹ ہے۔ اس میں سی سی ٹی وی کی تنصیب، مجرمانہ واقعات کے زیادہ واقعات والے علاقوں کی نشاندہی کر کے پولیسنگ کی پیش گوئی کے اقدامات شامل ہیں۔
یہ نظام ابتدائی طور پر لاہور میں لگایا گیا تھا اور اب تک کم از کم 6 دیگر شہروں (اسلام آباد، بہاولپور، ملتان، فیصل آباد، گوجرانوالہ، راولپنڈی) میں توسیع کے منصوبوں کے ساتھ موجود ہے۔

PSCA

جس دائرہ کار کے تحت کام کرتا ہے، کراچی میں بھی 10,000 کیمروں کی
نصب کی اطلاعات ہیں اور ان کے رہنمایانہ اصول کے طور پر سیکیورٹی کے مطلوبہ عنصر کو دیکھتے ہوئے یہ نصب کیا گیا ہیں ۔ یہ ممکن ہے کہ برسوں کے دوران تیار کردہ فوٹیج کے ڈیٹا بیس کو احتجاج کی نگرانی کے لیے استعمال کیا جا سکے۔

MOITT

کی طرف سے شروع کیے جانے والے پیشین گوئی والے پولیسنگ پروگراموں
کے علاوہ جرائم کو کم کرنے کی کوششوں میں ڈیجیٹلائزیشن کے لیے متعدد اقدامات بھی شروع کیے ہیں جیسے کہ ہوٹل آئی ایف آئی آر (فرسٹ انسٹنس رپورٹ) ،اور ٹریول آئی کے ساتھ ساتھ پولیس اسٹیشنوں کی وسیع پیمانے پر ڈیجیٹلائزیشن[15] کا اندراج اور شکایت کا میکانزم[16]

یہاں تشویش یہ ہے کہ ملک میں ذاتی ڈیٹا کا وسیع پیمانے پر ذخیرہ ہے اور اس ڈیٹا کو جمع اور استعمال کرنے کے ارد گرد کوئی قانون نہیں موجود اور ساتھ ہی میں اس ڈیٹا پر مبنی ڈیٹا بیسز کی پروسیسنگ کی دیکھ بھال نہیں کی جاتی۔

نگرانی کے خلاف اپنے آلات کی حفاظت کے لیے ایک گائیڈ

ڈیٹا لوکیشن تک رسائی کو بہتر طریقے سے کنٹرول کرنے کا طریقہ

میرے فون کا لوکیشن ڈیٹا کہاں محفوظ ہے؟

GPS یا موبائل نیٹ ورک لوکیشن کا استعمال کرتے ہوئے آپ کا فون دو اہم طریقوں سے اپنامقام تلاش کر سکتا ہے۔

---

[15] Muhammad Saleh Zaafir, “Crime analytics and smart policing to be implemented in Pakistan: Aminul Haq,” The News International, August 24, 2022, https://www.thenews.com.pk/print/984957-crime-analytics-and-smart-policing-to-be-implemented-in-pakistan-aminul-haq.

[16] Muhammad Shahzad, “Police stations across Punjab going digital,” March 12, 2017, https://tribune.com.pk/story/1353012/police-stations-across-punjab-going-digital.
Manzoor Ali, “Police dept digitises over 1.43m FIRs,” Dawn, October 7, 2018, https://www.dawn.com/news/1437332.

: GPS . 1

گلوبل پوزیشننگ سسٹم) سیٹلائٹ نیویگیشن کا استعمال کرتے ہوئے آپ کے فون کو بالکل درست طریقے سے تلاش کرتا ہے (چند میٹر کی حد کے اندر) اور آپ کے ہینڈ سیٹ کے اندر

GPS ۔چپ پر انحصار کرتا ہے

آپ جو فون استعمال کرتے ہیں یہ اس پر منحصر ہے۔ اپ کے جی پی ایس لوکیشن کا ڈیٹا اور یا گوگل کلاؤڈ یا کلاؤڈ کسی بھی ایپ کے ذریعے بھی جمع کیا جا سکتا ہے جسے آپ کے کسی بھی کلاؤڈ سروس پر اسٹور کیا جا سکتا ہے۔ اسے آپ کی استعمال کردہ

۔ایپس کے ذریعے بھی استعمال کیا جا سکتا ہے جن میں اپ کا لوکیشن ڈیٹا مانگا جاتا ہے

2:موبائل نیٹ ورک کا مقام :

موبائل نیٹ ورک لوکیشن (یا گلوبل سسٹم فار موبائل کمیونیکیشنز، جی ایس ایم لوکلائزیشن) آپ کے سیلولر نیٹ ورک پر انحصار کرتا ہے، اور آپ کے نیٹ ورک سے منسلک ہوتے ہی اس کا تعین کیا جا سکتا ہے (یعنی آپ کا فون آن ہے اور ایروپلین موڈ میں تو نہیں ہے) لیکن یہ جی پی ایس سے کم درستگی پر لوکیشن کی نشاندھی کرتا ہے۔

آپ کے تخمینی مقام کا تعین شہر میں چند درجن میٹر یا دیہی علاقوں میں سینکڑوں میٹر کی درستگی کے ساتھ کیا جا سکتا ہے۔ مقام کا ڈیٹا آپ کے نیٹ ورک فراہم کنندہ کے ذریعہ محفوظ کیا جاتا ہے۔

؟میرے مقام کے ڈیٹا یعنی لوکیشن ڈیٹا تک کیسے رسائی حاصل کی جا سکتی ہے

:آپ کے (فون) کے مقام تک رسائی حاصل کرنے کے لیے کئی طریقے استعمال کیے جا سکتے ہیں

: GPS.1

جی پی ایس لوکیشن ڈیٹا تک رسائی اس بات پر منحصر ہے کہ ڈیٹا کہاں محفوظ ہے۔ یہ ایک ''موبائل فون ایکسٹرکشن'' ڈیوائس کا استعمال کرتے ہوئے کیا جا سکتا ہے جو آپ کے فون میں پلگ ان ہوتا ہے اور اس پر ذخیرہ کردہ تمام ڈیٹا کو ڈاؤن لوڈ کرتا ہے بشمول ان مقامات کی تفصیلات جن کا آپ نے دورہ کیا ہے۔

اپ کے جی پی ایس ڈیٹا تک رسائی ڈیوائس ہیکنگ کے ذریعے بھی ممکن ہو سکتی ہے، ایک جدید تکنیک جس کے لیے ضروری نہیں کہ آپ کے فون تک جسمانی رسائی کی ضرورت ہو اور اسے دور سے بھی استعمال کیا جا سکتا ہے۔

اگرآپ کا جی پی ایس ڈیٹا آن لائن اکاؤنٹ میں بھی محفوظ ہے جیسے **Google Maps)** یا **Cloud**۔ تک رسائی حاصل کی جا سکتی ہے **(**

کلاؤڈ نکالنے والی ٹیکنالوجیز یا اس ڈیٹا کو اسٹور کرنے والی کمپنیوں سے قانونی درخواستوں کے ذریعے رسائی حاصل کی جا سکتی ہے۔

2:موبائل نیٹ ورک کی لوکیشن

آپ کے مقام کا ڈیٹا یعنی لوکیشن ڈیٹا پولیس آپ کے سروس فراہم کنندہ کے ذریعے رسائی حاصل کر سکتی ہے۔اس کا مطلب یہ ہے کہ پولیس کو آپ کے فون ہینڈ سیٹ تک رسائی کی ضرورت نہیں ہے تاکہ یہ معلوم کیا جا سکے کہ آپ احتجاج کے ایک خاص قربت میں تھے۔

اسی معلومات تک رسائی کا ایک اور ذریعہ ایک آئی ایم ایس آئی کیچر (جیسے
Stingray ۔بھی کہا جاتا ہے) کا استعمال کرنا ہے

ایک آلہ جو کسی مخصوص علاقے میں بند اور موبائل نیٹ ورک سے منسلک تمام موبائل فونز کو روکنے اور ٹریک کرنے
۔کے لیے تعینات کیا جاتا ہے

؟لوکیشن ڈیٹا کو بہتر طریقے سے کیسے کنٹرول کرسکتے ہیں

: GPS: 1
آپ کے مقام تک رسائی کو روکنے کا بہترین طریقہ یہ ہے کہ پہلے مقام کے ڈیٹا کی تخلیق کو محدود کیا جائے۔جی پی ایس کے معاملے میں، یہ اتنا ہی آسان ہو سکتا ہے جتنا آپ کے جی پی ایس کو بند کرنا (اکثر اسے مقام کی خدمات کہا جاتا ہے)۔ لیکن اس بات کو ذہن میں رکھیں کہ کسی بھی سابقہ مواقع کے مقام کا ڈیٹا جہاں آپ نے اسے آن کیا تھا وہ اب بھی قابل
۔رسائی ہو سکتا ہے

آپ کو اب بھی اپنے فون پرجی پی ایس استعمال کرنے کی ضرورت پڑ سکتی ہے، مثال کے طور پر اگر آپ چاہتے ہیں کہ کوئی دوست یا خاندانی رکن حفاظتی مقاصد کے لیے آپ کے مقام سے آگاہ ہو جب آپ احتجاج میں شرکت کرتے ہیں۔ اس صورت
۔میں اس معلومات کے پھیلاؤ کو کم کرنے کے لیے اپنے مقام تک رسائی کے لیے انفرادی ایپس کی اجازتوں کو چیک کریں
تمام ایپس کے لیے اپنے مقام تک رسائی کی اجازتوں کو ہٹانے سے اس ڈیٹا کو آن لائن اکاؤنٹ میں محفوظ ہونے سے روکا جا
۔سکتا ہے

آپ کو اپنے جی پی ایس ڈیٹا تک رسائی حاصل کرنے کے لیے کسی ایپ کی بالکل اشد ضرورت ہے، تو اس ایپ کی سیٹنگز کا معائنہ کریں تاکہ یہ یقینی بنایا جا سکے کہ آیا آپ کا مقامی معلومات آن لائن اسٹور کی جا رہی ہیں یا آپ کی ایپ میں پر مقامی طور پر،مثال کے طور پر اگر آپ گوگل اکاؤنٹ میں لاگ ان ہوتے ہوئے گوگل میپس استعمال کرتے ہیں تو آپ سیٹنگز
۔میں لوکیشن ہسٹری کو غیر فعال کرنا چاہیں گے تاکہ آپ کی لوکیشن ہسٹری آپ کے گوگل اکاؤنٹ میں محفوظ نہ ہو

اگر آپ نے اپنی لوکیشن سروسز کو آن کر کے تصویریں کھینچی ہیں، تو وہ مقام جہاں
(تصویر لی گئی تھی تصویر کے میٹا ڈیٹا (جسے ای ایکس ائی ایف ڈیٹا کہا جاتا ہے
میں شامل کیا جا سکتا ہے۔ تصویریں کھینچتے وقت مقامی ڈیٹا یعنی لوکیشن ڈیٹا کی خدمات کو آف کرلیں یا پھر بعد میں
۔ای ایکس ائی ایف ڈیٹا کو مٹانے کے لیے سافٹ ویئر یا ایپ استعمال کر سکتے ہیں

مثال کے طور پر، جب آپ تصاویر بھیجتے ہیں تو سگنل میسجنگ ایپ، ای ایکس ائی ایف
۔ ڈیٹا کو مٹا دیتی ہے اسی طرح، آپ کے وائی فائی یا بلوٹوتھ کو بند کرنا آپ کے فون کو ناپسندیدہ ایکسیس یعنی رسائی کے
۔پوائنٹس سے منسلک ہونے اور بالواسطہ مقام کی معلومات فراہم کرنے سے روک سکتا ہے

2: : موبائل نیٹ ورک کا مقامی ڈیٹا

جب موبائل نیٹ ورک کے مقامی ڈیٹا کی بات آتی ہے تو اس پر کنٹرول رکھنے کا واحد طریقہ یہ ہے کہ نیٹ ورک سے کنیکشن کو روکا جائے۔
آپ کے فون کو بند کرنے، ایروپلین موڈ میں، یا فیراڈے کیج میں رکھنے سے آپ کے موبائل نیٹ ورک سے رابطہ رک جائے گا جس سے جی ایس ایم جغرافیائی محل وقوع کے ڈیٹا تک رسائی کو ناممکن بنا دے گا۔ فیراڈے کیج کا استعمال یا اپنے فون کو بند کرنا کسی بھی فون نیٹ ورک سے تمام قسم کے کنیکشن کو روکتا ہے۔ جبکہ صرف ہوائی جہاز کے موڈ کے استعمال کا مطلب یہ ہے کہ کچھ قسم کے کنکشن اب بھی بنائے جا سکتے ہیں (جیسے بلوٹوتھ یا جی پی ایس) **

پولیس آپ کی تصاویر، رابطوں اور دستاویزات تک کیسے رسائی حاصل کر سکتی ہے اور آپ اس رسائی کو بہتر طریقے سے کیسے کنٹرول کر سکتے ہیں؟

یہ سب کہاں ذخیرہ یا جمع ہوتا ہے؟

جب بھی آپ اپنا فون استعمال کرتے ہیں، آپ ڈیٹا بناتے ہیں، جیسے جب آپ تصاویر لیتے ہیں یا ویڈیوز ریکارڈ کرتے ہیں، جب آپ چلتے پھرتے نوٹس اور دستاویزات بناتے یا ان میں ترمیم کرتے ہیں اور جب آپ اپنی رابطہ ڈائریکٹری میں نئے نام اور نمبر شامل کرتے ہیں تو آپ ڈیٹا تیار کر رہے ہوتے ہیں۔
یہ تمام ڈیٹا ڈیڈیکیٹڈ ایپس کے ذریعے بنایا گیا ہے ۔ آپ کا کیمرہ اور فوٹو ایپس، سوشل میڈیا ایپس، نوٹس ایپس، اور آپ کے رابطوں کی ایپس، یہ کچھ مثالیں ہیں۔
یہ نوٹ کرنا ضروری ہے کہ جب آپ اپنے فون پر کوئی فائل بناتے ہیں تو زیادہ تر آپ 'میٹا ڈیٹا' بھی تیار کریں گے جو اس کے ساتھ جوڑا جاتا ہے (مثال کے طور پر کسی تصویر میں میٹا ڈیٹا ہوگا جیسے کہ وہ وقت اور مقام جب اسے شوٹ کیا گیا تھا)۔ یہ میٹا ڈیٹا اتنا ہی ظاہر کر سکتا ہے اگر آپ خود تصویر سے زیادہ افشاں نہ کریں۔
یہ تمام ڈیٹا آپ کے فون کی اندرونی میموری (بشمول کوئی بیرونی میموری منسلک ہے جیسے کہ مائیکرو ایس ڈی کارڈ)، یا کلاؤڈ پر، یا اگر آپ بیک اپ کے طور پر کوئی کلاؤڈ سروسز استعمال کر رہے ہیں تو دونوں پر محفوظ کیا جائے گا۔

پولیس تصاویر، رابطوں اور دستاویزات تک کیسے رسائی حاصل کر سکتی ہے؟

پولیس کے پاس اس ڈیٹا تک رسائی حاصل کرنے کے چند طریقے ہیں، اور یہ اس پر منحصر ہے کہ ڈیٹا کیسے جمع کیا جاتا ہے :

اگر آپ اپنے تمام ڈیٹا کو مقامی طور پر اپنے فون پر اسٹور کرتے ہیں تو اس تک ایک موبائل فون ایکسٹریکشن ڈیوائس کا استعمال کرتے ہوئے رسائی حاصل کی جا سکتی ہے جو آپ کے فون سے منسلک ہوتا ہے اور اس میں محفوظ کردہ تمام ڈیٹا کو ڈاؤن لوڈ کرتا ہے۔ پولیس کو آپ کے فون تک جسمانی رسائی کی ضرورت ہوگی۔

ڈیوائس ہیکنگ ایک جدید تکنیک ہے جو آپ کے فون میں ڈیٹا کی ایک خاص مقدار تک رسائی فراہم کرتی ہے، لیکن ضروری نہیں کہ یہ کافی ہو۔ موبائل فون نکالنے کے برعکس، ہیکنگ کے لیے ضروری نہیں کہ آپ کے آلے تک جسمانی رسائی کی ضرورت ہو۔ اس کا مطلب ہے کہ یہ طریقہ احتجاج سے پہلے یا بعد میں کسی بھی وقت استعمال کیا جا سکتا ہے۔

اگر آپ کسی بھی کلاؤڈ سروسز (مثال کے طور پر آئی کلاؤڈ، ڈراپ باکس یا گوگل ڈرائیو)کا استعمال کرتے ہوئے اپنی تصاویر، دستاویزات اور رابطوں کو ہم آہنگ کر رہے ہیں تو پولیس آپ کی اجازت یا علم کے بغیر اس معلومات تک رسائی کے لیے 'کلاؤڈ ایکسٹریکشن' کے ٹولز کا استعمال کر سکتی ہے، یا وہ کلاؤڈ سروس فراہم کرنے والے سے قانونی درخواست کر سکتے ہیں۔

آپ کی تصاویر، رابطے اور دستاویزات تک رسائی کے خطرے کو کیسے محدود کیا جائے۔

کلاؤڈ ایکسٹریکشن کی تکنیکوں کے ذریعے نشانہ بننے سے بچنے کے لیے آپ کو کلاؤڈ سروسز کو مکمل طور پر استعمال کرنے سے گریز کرنا ہوگا۔اگر کلاؤڈ سروسز کو مکمل طور پر ترک کرنے سے آپ کے لیے بہت زیادہ دقت طلب عمل ہے، تو کلاؤڈ پر حساس مواد اپ لوڈ نہ کرنے پر غور کریں۔ ایپس کی سیٹنگز اور فیچرز کا جائزہ لینا بھی آپ کو یہ یقینی بنانے کا ایک اچھا طریقہ ہے کہ آپ کو معلوم ہے کہ آپ کے فون پر
کس ڈیٹا کا آن لائن بیک اپ لیا جا رہا ہے (مثال کے طور پر واٹس ایپ کے بیک اپس کو **Google Drive** اسٹور کیا جا سکتا ہے۔ اس لیے کیونکہ آپ کے واٹس ایپ پیغامات کو بیک اپ کرتا ہے۔ اینڈ انکرپٹڈ، کلاؤڈ ایکسٹریکشن ٹولز کا استعمال کرتے ہوئے ان پیغامات تک آپ کے گوگل ڈرائیو بیک اپ سے اب بھی رسائی حاصل کی جا سکتی ہے۔

تاہم، آلہ استعمال کے طور پر آپ کے پاس اس ڈیٹا پر کچھ کنٹرول ہوتا ہے جسے آپ پہلے تخلیق کرتے ہیں اور کہاں جمع کیا جاتا ہے۔ آپ کے فون میں آپ کے بارے میں کیا معلومات موجود ہیں اس کی اچھی طرح سمجھ رکھنے کا مطلب یہ ہے کہ اگر آپ کے فون پر ایسے ٹولز استعمال کیے جائیں تو آپ کو اس بات کا زیادہ امکان ہے کہ آپ کس ڈیٹا تک رسائی حاصل کر رہے ہیں۔
اس بات کو یقینی بنانا کہ آپ کے فون کا مواد انکرپٹڈ ہے اور یہ کہ آپ کا آپریٹنگ سسٹم اور ایپس اپ ٹو ڈیٹ ہیں موبائل فون نکالنے اور ڈیوائس ہیک کرنے کے کچھ طریقوں سے محفوظ ہو جائیں گے۔

ٹیکسٹ میسجز/فون کالز:
روایتی سیل فون مواصلات سیلولر نیٹ ورک پر ہوتے ہیں۔ آپ عام طور پر ٹیکسٹ میسج اور فون کال ایپس کے ذریعے ان تک رسائی حاصل کرتے ہیں جو آپ کے فون پر معیاری کے طور پر فراہم کی جاتی ہیں۔ اگرچہ فون کالز کہیں بھی محفوظ نہیں ہوتی ہیں لیکن ٹیکسٹ پیغامات مقامی طور پر آپ کے اور وصول کنندہ کے آلات پر محفوظ کیے جاتے ہیں۔ وہ نیٹ ورک فراہم کنندہ کے ذریعہ عارضی طور پر بھی جمع کیا جا سکتا ہے۔

پیغام رسانی کی ایپس:
پیغام رسانی کے پلیٹ فارمز انٹرنیٹ پر کافی حد تک محفوظ مواصلت کو فعال کرتے ہیں۔ آپ جو ایپ استعمال کرتے ہیں اس پر منحصر ہے کہ آپ کے پیغامات مقامی طور پر آپ کے اور وصول کنندہ کے فون پر، سروس فراہم کنندہ کے سسٹمز

پر، اور ممکنہ طور پر آن لائن بھی محفوظ کیے جا سکتے ہیں۔ کچھ میسجنگ ایپس بیک اپ سلوشن بھی پیش کرتی ہیں جو آن لائن یا مقامی طور پر اسٹور کیے جائیں گے۔ مختلف میسجنگ ایپس بھی مختلف پروٹوکولز پر انحصار کرتی ہیں جس کا مطلب ہے کہ کچھ میسجنگ ایپس کو دوسروں کے مقابلے میں مداخلت کا زیادہ خطرہ ہوتا ہے۔

سوشل نیٹ ورکس:
سیلف ہوسٹڈ سسٹمز والے نظاموں کے شاذ و نادر صورتوں کے علاوہ، سوشل نیٹ ورکنگ ایپس پر آپ کی کمیونیکیشنز سروس فراہم کنندگان کے ذریعے محفوظ کی جائیں گی۔

میرے مواصلات تک کیسے رسائی حاصل کی جا سکتی ہے؟

کچھ طریقے ہیں جن سے پولیس ڈیٹا تک رسائی حاصل کر سکتی ہے اس پر منحصر ہے کہ آپ نے اسے کہاں محفوظ کیا ہے۔

آپ کے فون پر محفوظ کردہ مواصلات تک رسائی حاصل کرنا (جیسے کہ ٹیکسٹ میسجنگ ایپ میں آپ کی گفتگو) ایک موبائل فون نکالنے ڈیوائس کے ذریعے کیا جا سکتا ہے جسے آپ کے فون سے منسلک کیا جا سکتا ہے تاکہ اس پر ذخیرہ کردہ تمام ڈیٹا کو ڈاؤن لوڈ کیا جا سکے۔

اس طرح کی رسائی ڈیوائس ہیکنگ کے ساتھ بھی ممکن ہو سکتی ہے ایک ایسی تکنیک ہے جس کے لیے آپ کے فون تک جسمانی رسائی کی ضرورت نہیں پیش آ سکتی ہے۔

اگر آپ کے مواصلات سروس فراہم کرنے والے یا سوشل نیٹ ورک (جیسے میسنجر، ٹیلیگرام، انسٹاگرام **(TikTok**، پر انحصار کرتے ہیں، تو پولیس آپ کی رضامندی یا علم کے بغیر 'کلاؤڈ ایکسٹریکشن' ٹیکنالوجیز کے ذریعے رسائی حاصل کر سکتی ہے۔ اسی تکنیک کو آپ کے مواصلات کے بیک اپ تک رسائی حاصل کرنے کے لیے بھی استعمال کیا جا سکتا ہے (جیسے
WhatsApp پر **Google Drive/iCloud** بیک اپ)۔
اگر سوشل نیٹ ورکس پر آپ کی کچھ کمیونیکیشنز عوامی ہیں (مثلاً کسی کھلے فیس بک گروپ پر شیئر کی گئی ہیں) تو پولیس ان تک رسائی کے لیے سوشل میڈیا انٹیلی جنس ٹولز بھی استعمال کر سکتی ہے۔ **(SOCMINT)**
"آپ کے ٹیکسٹ پیغامات اور فون کالز کو پولیس ایک " آئی ایم ایس آئی کیچر کا استعمال کرتے ہوئے رسائی حاصل بھی کر سکتی ہے ، ریکارڈ بھی کر سکتی ہے اور اس میں مداخلت بھی کر سکتی ہے۔ یہ ایک آلہ ہے جو کسی مخصوص علاقے میں نیٹ ورک سے منسلک تمام موبائل فونز کو ٹریک کرنے کے لیے تعینات کیا جاتا ہے۔

آپ کے ٹیکسٹ پیغامات تک آپ کے سروس فراہم کنندہ کو نشانہ بناتے ہوئے قانونی عمل کے ذریعے بھی رسائی حاصل کی جا سکتی ہے۔ اسی طرح کے قانونی عمل کو ان کمپنیوں سے ڈیٹا کی درخواست کرنے کے لیے استعمال کیا جا سکتا ہے جو آپ کے مواصلات کی میزبانی کر سکتی ہیں (جیسے فیس بک)۔

مواصلات تک رسائی کے خطرے کو کیسے محدود کیا جائے؟

خطرات کو محدود کرنا آپ کی معلومات کی مقدار اور قسم کو کنٹرول کرنے سے شروع ہوتا ہے کہ آپ کس کے ساتھ اور کس ذریعے سے اسے شیئر کرتے ہیں۔

انتہائی حساس معلومات کا اشتراک کرتے وقت، ذاتی طور پر ملاقات کر کہ بات کرنے پر غور کریں۔

اگر سیلیولر نیٹ ورکس کی کمزور سیکیورٹی کے پیش نظر ذاتی طور پر ملاقات ایک آپشن نہیں ہے تو حساس معلومات کا اشتراک کرنے کے لیے محفوظ چینلز جیسے اینڈ ٹو اینڈ انکرپٹڈ میسجنگ ایپس کے استعمال پر غور کریں۔

لیکن یہ بات ذہن میں رکھیں کہ اگر آپ اپنی کسی بھی میسجنگ ایپس کے لیے کلاؤڈ بیک اپ استعمال کرتے ہیں تب بھی کلاؤڈ ایکسٹریکشن ٹولز کا استعمال کرتے ہوئے مواد تک رسائی حاصل کی جا سکتی ہے۔

مظاہرین جن سے آپ کسی آنے والے مظاہرے کے لئے رابطے میں ہیں، ان کی شناخت کی توثیق کریں جیسے کہ آپ ان سے ایک مختلف مواصلاتی چینل کے ذریعے بات کر کے (مثلاً انہیں دوسرے پلیٹ فارم پر پیغام بھیجنا، یا انکرپٹڈ ای میل پر، یا ویڈیو کال کے ذریعے)ان کی شناخت کو یقینی بنا لیں۔

منفرد شناخت کنندہ: وہ کیا ہیں اور کہاں محفوظ ہیں؟

- جن تک پولیس آپ کی شناخت کے لیے رسائی حاصل کر سکتی ہے آپ کے فون اور آپ کے سم کارڈ میں آپ کے بارے میں منفرد شناخت کار ہوتے ہیں۔

آئی ایم ایس آئی(انٹرنیشنل موبائل سبسکرائبر آئیڈینٹی) آپ کے سم کارڈ سے منسلک ایک منفرد نمبر ہے۔ یہ تبدیل نہیں ہوتا، چاہے آپ سم کارڈ کو کسی دوسرے فون میں ڈال دیں۔

اگر آپ کے پاس موبائل فون سبسکرپشن ہے تو آئی ایم ایس آئی ذاتی معلومات جیسے کہ آپ کا نام اور پتہ سے منسلک ہوگا۔

آئی ایم ای آئی (بین الاقوامی موبائل آلات کی شناخت) ایک منفرد نمبر ہے جو آپ کے فون (آلے) کی شناخت کرتا ہے۔ لہذا اگر آپ اپنا فون تبدیل کرتے ہیں تو آپ کے پاس ایک آئی ایم ای آئی ہوگا۔

آئی ایم ایس آئی اور آئی ایم ای آئی کو ماہر ٹول کے بغیر آسانی سے تبدیل نہیں کیا جا سکتا، اور انہیں آپ کے بارے میں معلومات (جیسے نام، پتہ) یا آپ کے آلے (جیسے برانڈ، ماڈل) سے منسلک کیا جا سکتا ہے۔

اشتہاراتی شناخت: اشتہاراتی شناخت کنندگان آئی ایم ایس آئی اور آئی ایم ای آئی
سے مختلف ہیں کیونکہ وہ وقت کے ساتھ بدل سکتے ہیں۔ اشتہاری آئی ڈی
کا استعمال ایپس اور ویب سائٹس میں مشتہرین کے ذریعے آپ کی آن لائن منفرد شناخت کرنے اور ٹارگٹڈ ایڈورٹائزنگ
جیسی خدمات پیش کرنے کے لیے کیا جاتا ہے۔ اشتہاراتی آئی ڈیز براہ راست آپ کی ذاتی معلومات (مثلاً آپ کا نام) سے
منسلک نہیں ہوتی ہیں لیکن آپ کے بارے میں دیگر افشا کرنے والے ڈیٹا (مثلاً جغرافیائی محل وقوع، استعمال شدہ ایپس،
آپ کے فون کے آپریٹنگ سسٹم کے ذریعے تیار **ID** ملاحظہ کی گئی ویب سائٹس وغیرہ) سے منسلک ہو سکتی ہیں۔ اشتہار
۔کیا جاتا ہے، اور عام طور پر آپ کے فون کی سیٹنگز میں نظر آتا ہے۔ اسے دستی طور پر تجدید کیا جا سکتا ہے

:دیگر شناخت کنندگان
آپ کے فون میں کچھ دوسرے اجزاء ہیں جن میں قیاسی طور پہ عالمی سطح پر منفرد شناخت کار ہیں،جیسے کہ آپ کے
وائے فائے کا میک ایڈریس ، یا آپ کے بلوٹوتھ ماڈیول کے لیے
- BD_ADDR

؟منفرد شناخت کنندگان تک کیسے رسائی حاصل کی جا سکتی ہے

آپ کا آئی ایم ایس آئی اور آئی ایم ای آئی پولیس ایک آئی ایم ایس آئی کیچر کے ذریعے حاصل کر سکتی ہے۔ یہ ایک آلہ ہے
جو تمام موبائل
فونز کو ٹریک کرنے کے لیے تعینات کیا جاتا ہے جو اس کے آس پاس کے نیٹ ورک سے آن اور منسلک ہوتے ہیں۔ ایک بار
جب اس شناخت کنندہ کو روک لیا جاتا ہے، تو اس کا استعمال آپ کے بارے میں ذاتی معلومات کی بازیافت کے لیے کیا جا
۔سکتا ہے

آپ کے اشتہاراتی آئی ڈی تک آپ کے فون پر موجود ایپس اور ویب سائٹس تک رسائی
حاصل کی جا سکتی ہے۔ اگرچہ یہ براہ راست آپ کی ذاتی معلومات (مثلاً آپ کا نام اور پتہ) سے وابستہ نہیں ہے، لیکن یہ
آپ کے مقام جیسے دوسرے ڈیٹا سے منسلک ہو سکتی ہے۔ کچھ ڈیٹا بروکرز فون سے بڑی مقدار میں ڈیٹا حاصل کرتے ہیں
اور اسے پولیس کو فروخت کرتے ہیں، بشمول
.Ad ID

دیگر منفرد شناخت کنندگان جیسے آپ کا میک
ایڈریس وائی فائی ہاٹ سپاٹ کے ذریعے جمع کیا جا سکتا ہے لیکن اسے ذاتی معلومات کے ساتھ جوڑنا کہیں زیادہ مشکل ہے
جو آپ کی شناخت کے لیے استعمال ہو سکتی ہے، اور حالیہ آئی او ایس اور
۔اینڈرائیڈ ریلیزز آپ کے میک ایڈریس کو ایک سے منسلک کرنے پر دھوکہ دیں گی۔ نیا، نامعلوم نیٹ ورک

مظاہروں میں پولیس کی نگرانی کے سلسلے میں آپ کے ڈیٹا کے حقوق سے متعلق حقائق کا پرچہ

2016) پریوینشن آف الیکٹرانک کرائمز ایکٹ

(2) 35 سیکشن آلات اورڈیٹا سے نمٹنے والے افسران کو ہدایت دیتا ہے کہ
ا) تناسب کے ساتھ کام کریں ۔
ب) کسی بھی معلوماتی نظام کی رازداری کے تحفظ کے لیے اقدامات کریں جس میں انہیں تلاش کرنے اور ضبط کرنے کی طاقت کا استعمال کرتے ہوئے ان تک رسائی حاصل ہے۔

سیکشن 36 افسران کو ہدایت کرتا ہے کہ کس طرح ضبط کیے گئے انفارمیشن سسٹمز سے نمٹا جائے جس میں یہ درج کرنا شامل ہے کہ کون سی اشیاء ضبط کی گئی ہیں اور انفارمیشن سسٹم اور ڈیٹا کے مالک یا مالکان کو ان اشیاء کی فہرست فراہم کرنا ہے۔

سیکشن 41 معلومات کی رازداری سے بات کرتا ہے اور کسی بھی شخص، سروس فراہم کرنے والے یا مجاز تفتیشی افسر کے لیے تین سال قید اور/یا دس لاکھ روپے تک جرمانے کی سزا دیتا ہے جو بغیر رضامندی کے ڈیٹا افشاء کرتا ہے یا معاہدے کی ذمہ داریوں کی خلاف ورزی کرنے کے ارادے سے یہ جانتے ہوئے کہ وہ کسی بھی شخص کو نقصان یا فائدہ پہنچا سکتا ہے یا اس طرح کے مواد یا ڈیٹا کی رازداری سے سمجھوتہ کر سکتا ہے۔

رائٹ ٹو انفارمنشن
معلومات کا حق (آر ٹی آئی) قوانین

19A
آرٹیکل آئین پاکستان کے مطابق پاکستان میں اب چاروں صوبوں اور وفاقی سطح پر معلومات اور ریکارڈ تک رسائی کی اجازت دینے کے لیے آر ٹی آئی قوانین موجود ہیں۔ پاکستان میں اب چاروں صوبوں اور وفاقی سطح پر معلومات اور ریکارڈ تک رسائی کی اجازت دینے کے لیے آر ٹی آئی قوانین موجود ہیں۔

ہر شہری کو عوامی اہمیت کے تمام معاملات میں معلومات تک رسائی حاصل کرنے کا حق ہے جو کہ قانون کے ذریعہ عائد کردہ ضابطے اور معقول پابندیوں کے تابع ہو۔

2017 وفاقی: معلومات تک رسائی کا حق ایکٹ

2013 پنجاب: پنجاب ٹرانسپیرنسی اینڈ رائٹ ٹو انفارمیشن ایکٹ

2013 خیبر پختونخوا: کے پی رائٹ ٹو انفارمیشن ایکٹ

2016 سندھ: سندھ ٹرانسپیرنسی اینڈ رائٹ ٹو انفارمیشن ایکٹ

2021 بلوچستان: بلوچستان رائٹ ٹو انفارمیشن ایکٹ

افراد اور تنظیمیں معلومات کی درخواستیں کرنے کے لیے ہر دائرہ اختیار کے حوالے سے انفارمیشن کمشنرز سے رجوع کر سکتی ہیں۔ ان قانونی آلات میں اوور رائیڈنگ انتباہات اور مستثنیات میں معلومات کے افشاء کو محدود کرنا شامل ہے لیکن اگر یہ کسی جرم کے ارتکاب کا باعث بن سکتا ہے، کیس کی انکوائری میں رکاوٹ یا قومی سلامتی کے تحفظات کو متاثر کر سکتا ہے۔

احتجاجی مظاہرے میں پولیس افسران کی فوٹوگرافی

2017[17] میں پنجاب پولیس کے انسپکٹر جنرل کی جانب سے پنجاب کے تمام تھانوں میں موبائل فونز، لیپ ٹاپ اور کیمروں پر پابندی عائد کرنے کے لیے ایک پالیسی ہدایت جاری کی گئی تھی

لیکن ہمارے موجودہ علم کے مطابق کوئی واضح پالیسی یا قاعدہ موجود نہیں ہے جو پولیس افسران کی فوٹو گرافی کو مجرم قرار دیتا ہے۔ احتجاج چونکہ پبلک یعنی عوامی اجتماعات ہیں، اس لیے فوٹو گرافی پر پابندیاں آزادی اظہار کے تحفظات کے خلاف ہو سکتی ہیں۔
غیر متناسب طاقت کے استعمال کی طرف توجہ دلانے کے لیے پولیس افسران کی جانب سے استعمال کیے گئے غیر آئینی، کی فوٹو گرافی اور ویڈیو گرافک شواہد کو احتساب کا مطالبہ کرنے کے لیے ایک آلے کے طور ضرورت سے زیادہ سخت رویے[18] پر استعمال کرنے کے لیے ریکارڈ جا سکتا ہے۔
اس حقیقت سے قطع نظر کہ پولیس افسران کے طرز عمل کی تصاویر لینا، فلمانا یا کسی اور طرح سے ریکارڈ کرنا غیر قانونی نہیں ہے۔مظاہرین کو ان سرگرمیوں کو انجام دیتے وقت احتیاط برتنی چاہیے تاکہ حفاظت کو لاحق خطرات سے بچا جا سکے۔

نوٹ: عوامی طور پر ایسی کوئی معلومات دستیاب نہیں ہیں کہ پاکستان کے قانون نافذ کرنے والے ادارے ایم پی ای ٹولز کی تعیناتی کر رہے ہیں، تاہم ہم اس کی موجودگی کو عام تلاش اور اختیارات پر قبضے کی بنیاد پر خارج نہیں کر سکتے۔

[17] https://www.dawn.com/news/1353555
[18] https://www.dawn.com/news/1694624