अधिकारों के बदलते स्वरुप: इंटरनेट, डेटा और निजता

DIGITAL EMPOWERMENT foundation

अधिकारों के बदलते स्वरुप:
इंटरनेट, डेटा और निजता

अधिकारों के बदलते स्वरुपः इंटरनेट, डेटा और निजता

डिजिटल सशक्तिकरण फाउंडेशन द्वारा प्रकाशित और वितरित

लेखकः आशिफ इकबाल
संपादकः अनुष्का झा और तरुण प्रताप
संकल्पनाः अनुलेखा नंदी
समीक्षाः ओसामा मंज़र, शाम्भवी मदन और सना आलम
डिजाइन और चित्रणः शारदा केरकर

यह काम एक रचनात्मक कॉमन्स एट्रीब्यूशन 4.0 इंटरनेशनल लाइसेंस के तहत लाइसेंस प्राप्त है।

प्रकाशन का वर्षः 2020

डिजिटल एम्पावरमेंट फाउंडेशन
3 मंजिल, 44, कालू सराय, आईआईटी फ्लाईओवर के पास,
नई दिल्ली – ११० ०१६, भारत
दूरभाषः + 91–11–43322100
www.defindia.org
Email: def@defindia.net

इंटरनेट ने हमारे जीवन को हर ढंग से बदल दिया है. हमारे बा. त–चीत से लेकर हमारे सोचने–समझने के अंदाज तक को.

जैसा की होता आया है के हर तकनीक, हर बदलाव अपने फायदों के साथ–साथ नए खतरों को भी जन्म देती है.

डेटा हमारे जीवन–व्यापन को पहले भी अलग–अलग ढंग से प्रभा. वित करता रहा है, अभी भी कर रहा है और आने वाले समय में और अधिक करेगा.

ऐसे में इसके बारे में समझना कहीं अधिक महत्वपूर्ण हो जाता है. यह एक प्रयास है डेटा के बारे में आपकी राय को परिपक्व बनाने की और उससे जुड़े अधिकारों को समझाने की.

क्या आप सोशल मीडिया जैसे फेसबुक, व्हाट्सएप इत्यादि का उपयोग करते हैं?

सोशल मीडिया जैसे व्हाट्सएप, इन्स्टाग्राम, टिकटोक, फेसबुक इत्यादि हम सब उपयोग करते हैं. अपनी फोटो भी शेयर करते हैं. दोस्तों की फोटो पसंद करते हैं, कमेंट भी करते है. हम बहुत से पेज भी पसंदध्फॉलो करते हैं. मनोरंजन से लेकर ख़बर तक के लिए. अलग–अलग जानकारियों के लिए भी अलग–अलग पेज फॉलो करते हैं.

प्रचार प्रचार प्रचार

आप ने देखा है, जब फेसबुक उपयोग कर रहे होते हैं तो अलग. –अलग प्रचार भी आते रहते हैं. मैंने तो देखा है. आप ने भी देखा होगा. आप ने कभी ध्यान दिया है कि वही प्रचार क्यूँ आते रहते हैं जो हमें पसंद हैं. जो हम देखना चाहते हैं. मैंने तो देखा है कि जो मैं खोजने का प्रयास करता हूँ गूगल पर, अमेजन पर, फ्लिप्कार्ट या पेटीएम् इत्यादि पर, उसी के प्रचार अक्सर मेरे फेसबुक पर आते हैं. आप भी ध्यान दीजियेगा, ऐसा ही कुछ होता है.

अगर ध्यान देंगे तो ये भी सोचियेगा कि ऐसा कैसे होता है. फेसबुक या किसी भी सोशल मीडिया या आप के स्मार्टफोन पर की गयी कोई भी गतिविधि डेटा के रूप में एकत्रित की जाती हैं. आप जो साझा करते हैं, जो पसंद करते हैं, जो पढ़ते हैं सभी डेटा के रूप में कंप्यूटर में बिछे जाल में एकत्रित किये जाते हैं और उसे संशोधित किया जाता है. जो आप को दिखता है, जो प्रचार आते हैं, जो विडियो आते हैं, सब का आधार वही डेटा है. एकत्रित डेटा का उपयोग आपके जीवन व्यापन को प्रभावित करने के लिए किया जाता है.

डेटा

1. डेटा आप के द्वार दी गयी जानकारी है.

2. डेटा को एक ऐसे रूप में संग्रहित किया जाता है कि उसे संसाधित किया जा सके.

3. डेटा का उपयोग कर के आप के द्वारा लिए जाने वाले फैसले को प्रभावित किया जा सकता है, और आपकी गतिविधि पर भी नजर रखी जा सकती है.

4. सोशल मीडिया पर आप जो पसंद करते हैं, जो देखते हैं, जो फॉलो करते हैं यह सभी गतिविधि डेटा के रूप में एकत्रित की जाती हैं.

5. बड़ी–बड़ी कंपनीयां डेटा का उपयोग अपने काम को बेहतर बनाने के लिए करती हैं.

तो क्या डेटा सिर्फ सोशल मीडिय से एकत्रित किये जाते हैं?

नहीं. डेटा, दरअसल में आपके द्वारा दी गयी जानकारी है. जानकारी एकत्रित करने की परंपरा कोई नयी नहीं. अलग–अलग समय में अलग–अलग माध्यमों से, अलग–अलग जानकारियाँ जमा की जाती रही हैं.

भारत में सब से पहले, अंग्रेजों के शासन काल में, कुल घरों की जानकारियाँ 1872 में इकट्ठा की गयी थी. धीरे–धीरे उस में अलग. –अलग जानकारियां इकठ्ठा की जाने लगी, जिसे हम जनगणना कहते हैं. 2001 में हुए जनगणना में, आप कहाँ रहते हैं, परिवार में कितने सदस्य हैं, क्या करते हैं, कितनी संपत्ति हैं, क्या सुख–सुविधायें हैं और लिंग, आयु इत्यादि की जानकारी इकठ्ठा की गयी थी. इन जानकारियों का अध्ययन करके सरकारें आगे की नीतियाँ बनाती हैं.

अब नये–नये माध्यमों से डेटा इकठ्ठा किये जा रहे हैं, जैसे आधार कार्ड, स्वास्थ्य कार्ड इत्यादि. आधार के लिए हमारे अंगूठे के निशान, धर्म, जाति इत्यादि के डेटा इकट्ठे किये जाते हैं. सरकार की तरफ से ये कहा जा रहा है कि योजनाओं का लाभ, लाभार्थी तक पहुँचाने के लिए आधार की आवश्यकता है.

तो क्या डेटा सिर्फ सोशल मीडिय से एकत्रित किये जाते हैं?

1. अलग–अलग समय में अलग–अलग माध्यमों से डेटा संग्रहित किये जाते रहे हैं.

2. जनगणना भी डेटा इकठ्ठा करने का तरीका है.

3. सरकार डेटा का उपयोग नीतियां बनाने में करती हैं.

4. सरकार अलग–अलग डेटा जैसे, स्वास्थ्य डेटा, कृषि डेटा, निजी डेटा–आधार के माध्यम से– इत्त्यादि को भी इकठ्ठा करती हैं.

5. तकनीक के बढ़ते प्रभाव से डेटा के दुरूपयोग के खतरे बढ़ते जा रहे हैं.

डेटा एकत्रित करने के माध्यम

अलग–अलग समय में अलग–अलग माध्यमों से डेटा संग्रहित किये जाते रहे हैं.

तो क्या निजी संस्थाएं भी डेटा एकत्रित करती हैं?

हाँ. निजी संस्थाएं भी बड़ी मात्राओं में डेटा एकत्रित करती हैं. ओला, उबर से लेकर पेटीएम और जोमेटो से कोई भी एप्लीकेशन जो हम स्मार्टफोन या कंप्यूटर में उपयोग करते हैं, सभी कंपनीयां कंप्यूटर में उलझे तारों और सर्वर की मदद से डेटा को एकत्रित करती हैं और संसोधित भी करते हैं.

डेटा बुनियादी तौर दो प्रकार के होते हैं.

1.व्यक्तिगत डेटा

यह वह जानकारी है जिससे किसी व्यक्ति की पहचान की जा सकती हो. अलग जानकारियों को इकठ्ठा करके भी अगर किसी व्यक्ति की व्यक्तिगत पहचान की जा सकती है तो वैसी जानकारी को व्यक्तिगत डेटा कहते हैं. जैसे आपका मोबाइल नंबर, आपका नाम, जन्म प्रमाण पत्र, वेतन इत्त्यादी.

2. गैर–व्यक्तिगत डेटा

गैर–व्यक्तिगत डेटा का अधिकतर हिस्सा, मौसम ऐप द्वारा एकत्र किए गए जलवायु रुझान, या कैब एप्प जैसे ओला, उबर और सोशल मीडिया जैसे फेसबुक, इन्स्टाग्राम इत्यादि द्वारा एकत्र किए गए और कम्प्यूटर पैटर्न जैसे अज्ञात डेटा शामिल हैं.

तो क्या निजी संस्थाएं भी डेटा एकत्रित करती हैं?

1. व्यक्तिगत डेटा से आपकी पहचान सीधे तौर पर की जा सकती है.

2. गैर–व्यक्तिगत डेटा से आपकी पहचान सीधे तौर पर नहीं की जा सकती है.

3. आपके द्वारा दी जाने वाली निजी जानकारी को व्यक्तिगत डेटा कहते हैं.

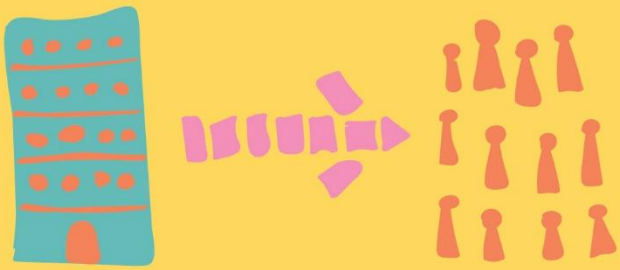
4. आपके द्वारा दी जाने वाली अव्यक्तिक डेटा को गैर व्यक्तिगत डेटा कहते हैं.

5. सोशल मीडिया से लेकर अलग–अलग एप्लीकशन जो आप उपयोग करते हैं वहां से दोनों तरह के डेटा इकठ्ठा करते हैं.

डेटा क्यूँ महत्वपूर्ण है?

डेटा का उपयोग, सरकार नीतियों को बनाने के लिए करती हैं. जानकारी एकत्रित करके उसका विश्लेषण किया जाता है, ताकि ये सुनिश्चित किया जा सके कि हर वर्ग का योजनाओं में प्रतिनिधित्व बराबरी से हो. बराबर की हिस्सेदारी दी जा सके. समानता लाने का प्रयास किया जा सके. बड़ी–बड़ी संसथान जानकारियों को इकठ्ठा करके ये सुनिश्चित करने का प्रयास करती है कि काम कैसे कुशलतापूर्वक किया जा सकता है. समय की बचत कैसे कि जा सकती है.

1. डेटा का उपयोग करके यह पता किया जा सकता है के आपको किस बात पर गुस्सा आता है, क्या पसंद हैं और क्या नापसंद हैं.



2. डेटा का उपयोग बिमा कंपनीयां से ले कर चॉक्लेट बेचने वाली कंपनीयां अपने ग्राहकों तक पहुँचने और उनको रुझान के लिए करती हैं.

3. डेटा का उपयोग सरकार नीतियों में सबकी हिस्सेदारी बराबरी से तय करने के लिए करती हैं.

4. डेटा का उपयोग यातायात सुविधाओं को बेहतर बनाने के लिए भी किया जाता है.

5. डेटा का उपयोग अपराध रोकने के लिए भी किया जाता है.

तो समस्या क्या है?

डेटा का उपयोग अच्छे कामों के साथ–साथ गलत कामों के लिए भी किया जा सकता है.

सरकार जो जानकारी इकठ्ठा कर रही है वो कितनी सुरक्षित है, यह एक बड़ा सवाल है. सोशल मीडिया और अन्य एप्लीकेशन के द्वारा इकठ्ठा की जा रही जानकारियों का उपयोग कौन और कैसे कर रहा है, यह भी अलग समस्या का रूप धारण कर रहा है.

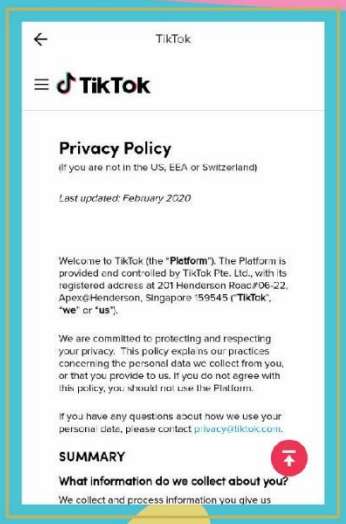
अभी हाल में ही अमेरिका में हुए चुनाव के बाद एक बड़ा बवाल खड़ा हो गया था. कैंब्रिज एनालिटिका नामक संस्था पर ये आरोप लगाया गया कि इस संस्था ने अमेरिकी चुनाव में फेसबुक के द्वारा इकठ्ठा किये गए जानकारियों का उपयोग करके मतदाताओं को प्रभवित किया है. भारत में भी कोबरा पोस्ट की रिपोर्ट के अनुसार पेटीएम् जैसी संस्था पैसे ले कर पक्षपात करते हैं.

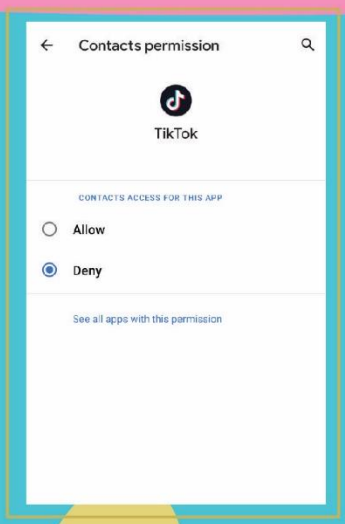
आप के द्वारा दी गयी जानकारी से ये पता किया जाता है कि आपको किस बात से अधिक प्रभावित हैं. राष्ट्रीय सुरक्षा को ले कर आप कितने चिंतित हैं. आप अर्थव्यवस्था को लेकर क्या सोच रहे हैं. आप कानून व्यवस्था को लेकर क्या सोच रहे हैं. आपको जो मुद्दे प्रभावित करते हैं, उसी के अनुसार आपके वोट देने कि सम्भावना है. आपको, आपके भय और पसंद के अनुसार वोट देने के लिए निजी तौर पर समझाया जा सकता है, और उस मुद्दे पर राजनितिक विमर्श खत्म करने के लिए ऐसा किया जाता है. लोकतंत्र की सबसे बड़ी ताकत मतदाताओं के हाथ में दी गयी शक्ति को समझा जाता रहा है, अगर ऐसा होता रहा तो लोकतंत्र नाम भर का रह जायेगा.

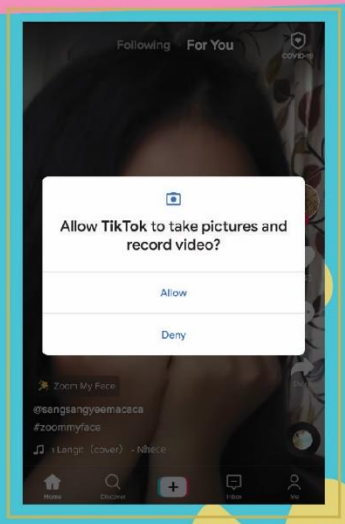
बड़ी–बड़ी कंपनीयां और राजनितिक पार्टी गठजोड़ करके मतदाता को प्रभावित करते रहेंगे. ठीक वैसे ही, ग्राहक की पसंद सबसे अधिक महत्वपूर्ण माना जाता रहा है, लेकिन तकनीकी होते इस दौर में यह कह पाना कठिन है कि यह ग्राहक की स्वतंत्र पसंद है या उसे अप्रत्यक्ष या प्रत्यक्ष रूप से प्रभावित किया गया है. यह सब उद्योगपति और सरकारों को अधिक शक्तिशाली बना देगा और जनता को और अधिक लचर.

तो क्या जानकारी हमारी सहमती से ली जाती हैं?

आपने कभी ध्यान दिया है कि जब आप कोई एप्लीकेशन अपने स्मार्टफोन में डाउनलोड करते हैं तो, एक बड़ी से कहानी लिख कर नीचे आपसे एक छोटे से आयातनुमा बॉक्स में टिक करने के लिए कहा जाता है. दरअसल जब आप ऐसे करते हैं तो एप्लीकेशन आप से सहमती लेता है कि आप के मोबाइल से कौन–कौन सी जानकारियां लेगा, और उस का उपयोग कैसे करेगा. इसे डेटा–सहमती कहते हैं.







डेटा–सहमति का अर्थ है, आप इस के लिए स्वतंत्र हैं कि आप अपने बारे कौन सी जानकारी साझा करना चाहते हैं कौन सी नहीं. अगर कोई आपके घर पर आपसे सवास्थ्य, शिक्षा या किसी भी प्रकार की जानकारी मांगने के लिए आता है तो आप उनसे पूछ सकते हैं हमारे बारे में आपको जानकारी लेने का क्या अधिकार है. उस जानकारी का आप क्या उपयोग करेंगे. ठीक उसी तरह इन्टरनेट पर दी जाने वाली जानकारियों पर भी आपका अधिकार है.

तो क्या जानकारी हमारी सहमती से ली जाती हैं?

1. डेटा के दुरपयोग होने के खतरे पहले से कहीं अधिक होते जा रहे हैं.

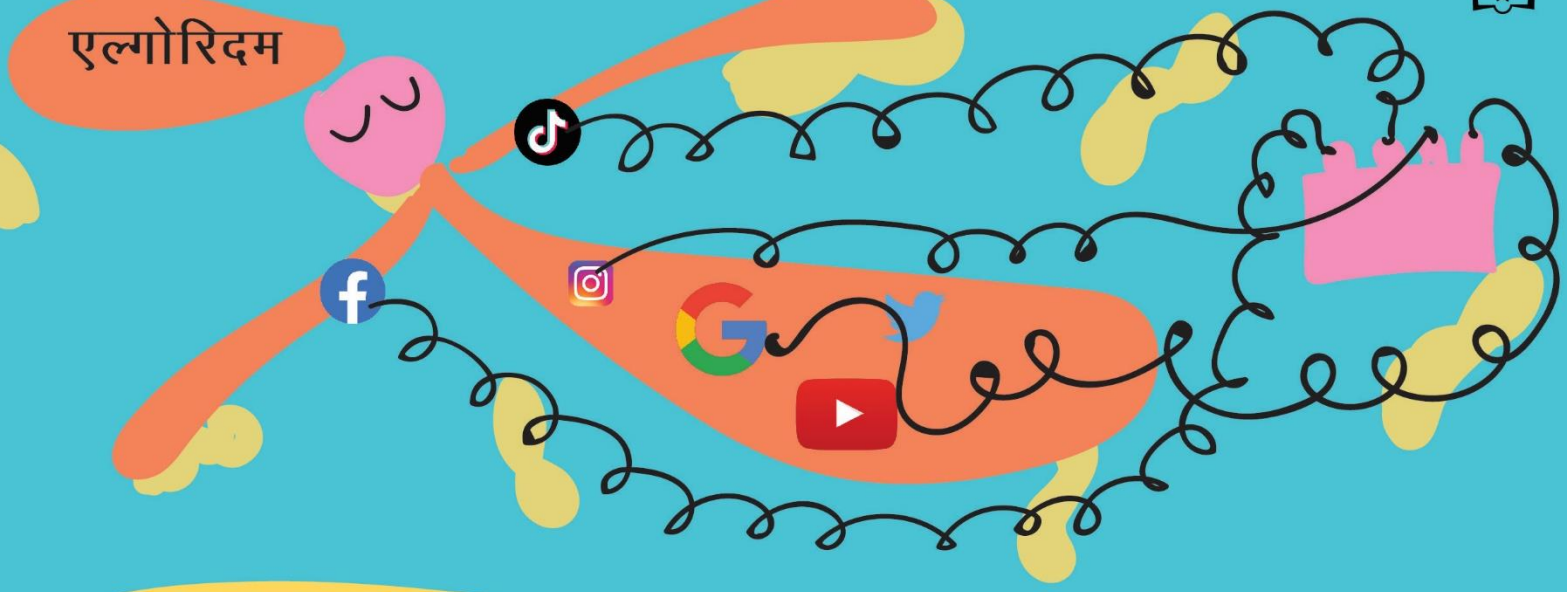
2. डेटा कि सुरक्षा को लेकर हर तरफ सवाल उठ रहे हैं.

3. डेटा से जानकारी जुटा कर चुनाव में मतदाताओं को प्रभावित किया जा सकता है.

4. आपका डेटा कौन और कैसे उपयोग कर रहा है इसको लेकर पा. रदर्शिता जरूरी है.

5. डेटा का सारा खेल आने वाले दिनों में आज से कहीं अधिक महत्वपूर्ण हो जायेगा.

एल्गोरिदम



सोशल मीडिया एल्गोरिदम प्रकाशित समय के बजाय प्रासंगिकता के आधार पर उपयोगकर्ताओं के फीड में दिखाने का तरीका है. सोशल मीडिया जैसे, फेसबुक, ट्विटर, इन्स्टाग्राम इत्यादि प्राथमिकता देते हैं कि उपयोगकर्ता अपने फीड में कौन सी सामग्री पहले देखता है. वह इसे प्राथमिकता दे कर वास्तव समय में दिखाने का प्रयास करते हैं. आपने देखा है कि जब आप कोई पेज पसंद करते हैं तो ठीक उसी प्रकार के पेज और अधिक सुझाव में आने लगते हैं. आप जैसी विडियो को पसंद करते है तो उसी प्रकार की और विडियो आने लगती हैं. आप जैसे फोटो पसंद करते हैं वैसे ही फोटो के सुझाव आने लगते हैं.

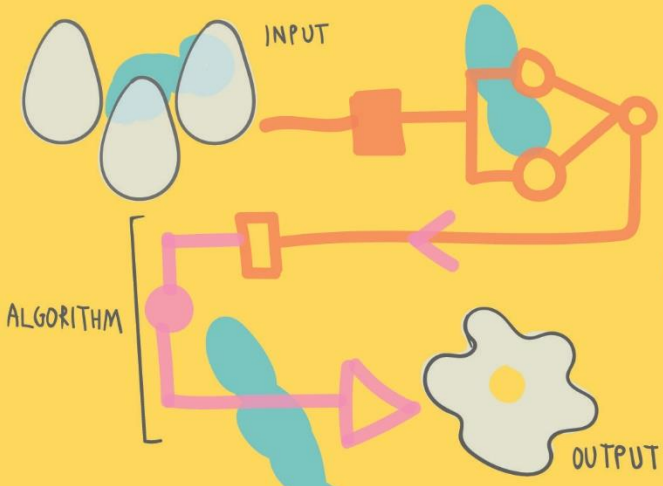
आप अगर राष्ट्रीय सुरक्षा को ले कर अगर कुछ सर्च करने का प्रयास करेंगे तो, हर जगह यूटयूब से ले कर फेसबुक तक पर आप राष्ट्रीय सुरक्षा से सम्बंधित कंटेंट आने लगेंगे. और इसके कारण, उस मुद्दे पर कोई सही समझ बनाना कठिन होता जाता है, बल्कि आपका पहले से जो विश्वास है उसे और दृढ होने कि उम्मीद अधिक है. आप ऐसे में, जब किसी ख़बर को देखते हैं तो उसके एक पक्ष को ही समझ पाते हैं, दूसरा पक्ष जानना कठिन हो जाता है.

एल्गोरिदम आपके आस–पास कभी न दिखने वाला घेरा बना देता है. हम अलग–अलग आभासी समूहों में बंटते चले जा जा रहे हैं. यह घेरा नए प्रकार का समुहिकीकरण कर रहा है, और इसके कारण फेक न्यूज से लेकर ध्रुविकरण करना आसान हो जाता है. इस सब का आधार आपके द्वारा एकत्रित की गयी जानकारी है.

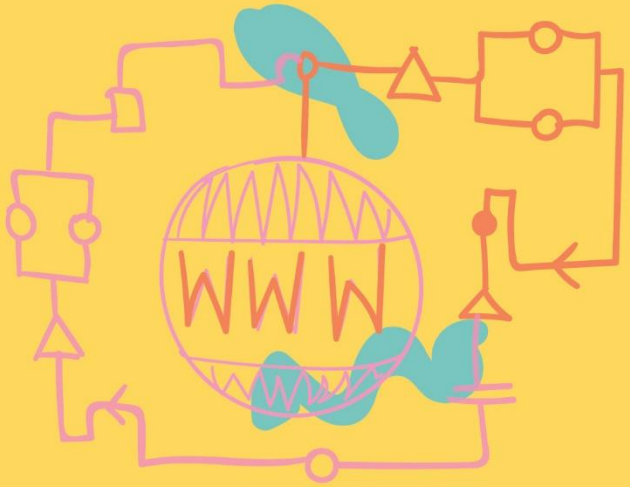
सोशल मीडिया से लेकर हर एप्लीकेशन को ये पता है कि आप क्या पसंद करते हैं, क्या नहीं. आपके मोबाइल अलार्म को पता है कि आप कब जगते हैं. आपके गूगल मैप को पता है कि आप कौन सा रास्ता कब लेते हैं. आपके गूगल असिस्टेंट को आपकी आवाज से पता है के आप कब गुस्से में होते हैं. स्विगी और जोमटो ये पता है कि आप कब और क्या खाते हैं.

एल्गोरिदम

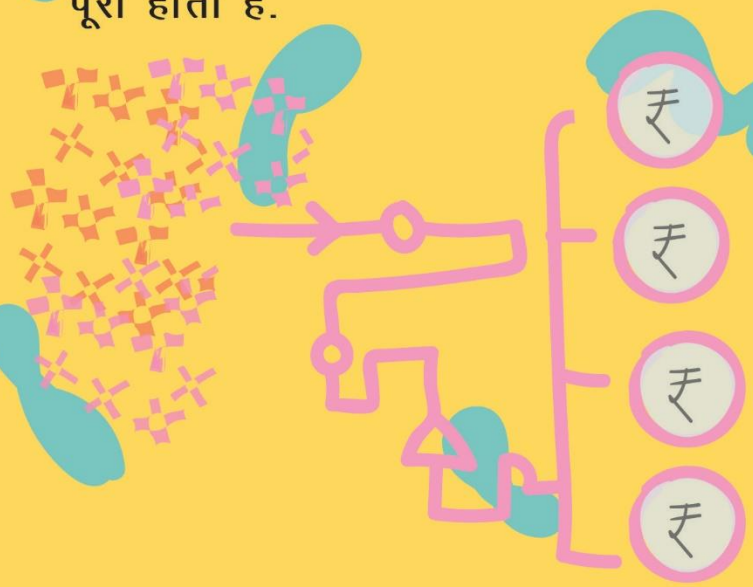
1. जिस विषय में आपकी रूचि अधिक होगी, एल्गोरिदम उसे आपको जल्द दिखाने का प्रयास करता है.



2. एल्गोरिदम का उद्देश्य हर चीज का अनुकूलन करना है. वे जीवन को बचा सकते हैं, चीजों को आसान बना सकते है.



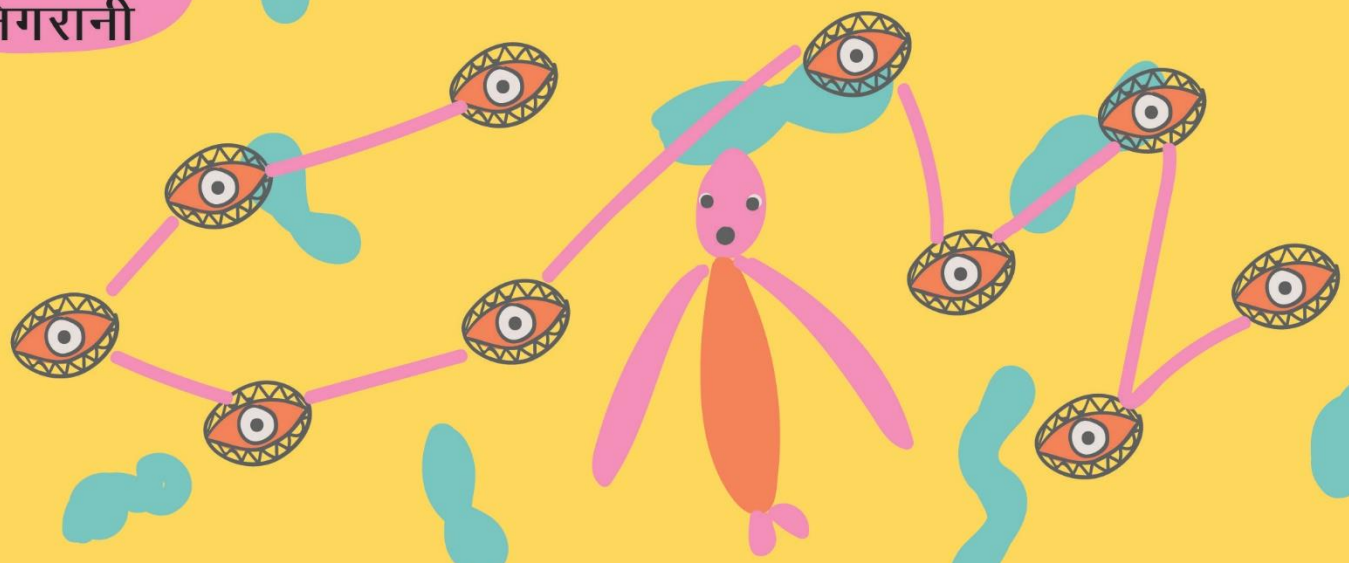
3. इंटरनेट एल्गोरिदम पर चलता है और सभी ऑनलाइन खोज उनके माध्यम से पूरी होती है.



4. एल्गोरिदम का उपयोग बड़े पैमाने पर हो रहा है क्योंकि व्यवसायों और सरकारों द्वारा बड़े पैमाने पर डेटा अनुग्रहित और विश्लेषित किया जा रहा है.

5. एल्गोरिदम आपके सामने एक आभासी घेरा बनाता है, जिसके कारण झूठ और प्रोपोगैंडा का फैलाना आसान होता जा रहा है.

निगरानी



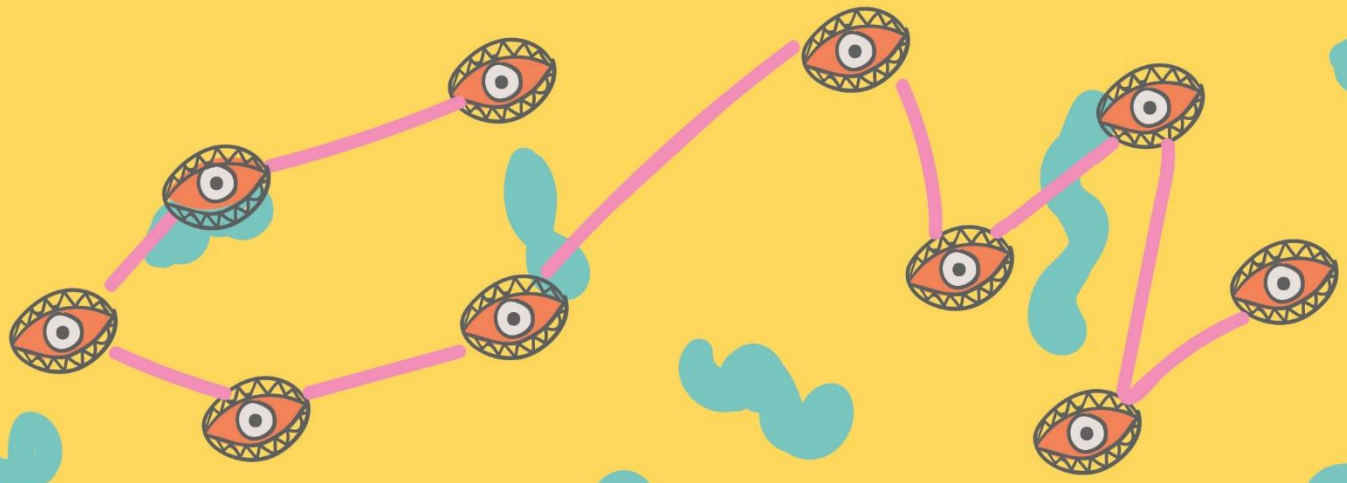
सार्वजनिक और निजी स्थानों की निगरानी और लोगों की पहचान करने के लिए अलग–अलग कैमरा का उपयोग किया जाता है. ब्ब्ज्ट (जिसे क्लोज्ड–सर्किट टेलीविजन या सीसीटीवी के रूप में भी जाना जाता है) का दुनिया भर में सार्वजनिक और निजी स्थानों की निगरानी के लिए उपयोग किया जा रहा है. क्या आपने कभी सोचा है कि ये जानकरियां जो इकट्ठी की जा रही हैं, वह कौन देख रहा है. वह जानकारियां कितनी सुरक्षित हैं.

निगरानी रखने से क्राइम रोकने में सहायता हो सकती है. सूरत से लेकर आंध्रप्रदेश में, अलग जानकारियों को इकठ्ठा करके पुलिस हिंसा रोकने के प्रयास कर रही है.

आधार कार्ड में हम सब की फोटो से ले कर आँखों की पुतली तक का डेटा सरकार ने इकठ्ठा कर रखा है, तकनीक के माध्यम से ब्ब्ज्ट में कैद आपकी गतिविधि को आधार से जोड़ कर आप पर नजर हर वक्त रखी जा सकती है. डेटा का उपयोग करके निगरानी रखने के कारण अलग तरह के भेदभाव सामने आ सकते हैं.

अगर किसी मध्य या कम आय वाले क्षेत्र में मशीन बताती है कि हिंसा होने की सम्भावना अधिक है, तो उस क्षेत्र के लोगों को अधिक निग. रानी में रहना पड़ेगा. कुछ लोगों जो हिंसा करते हैं, उनके लिए उस क्षेत्र में रहने वाले सभी की निजिता प्रभावित होगी. उस क्षेत्र में रहने वाले बच्चों के मानसिक विकास पर प्रभाव पड़ेगा.

हिंसा के नाम पर नयी मशीनों का उपयोग करके सोशल मीडिया पर निगरानी रखी जा रही है. सोशल मीडिया पर हिंसात्मक कंटेंट को रोकने को लिए निगरानी रखी जा रही है. पुलिस भी वहां निगरानी रखने का प्रयास कर रही है. निजिता को लेकर सवाल खड़े हो रहे हैं. जानकारी के सुरक्षा के सवाल खड़े हो रहे हैं. उनके उपयोग को लेकर प्रश्न खड़े हो रहे हैं.



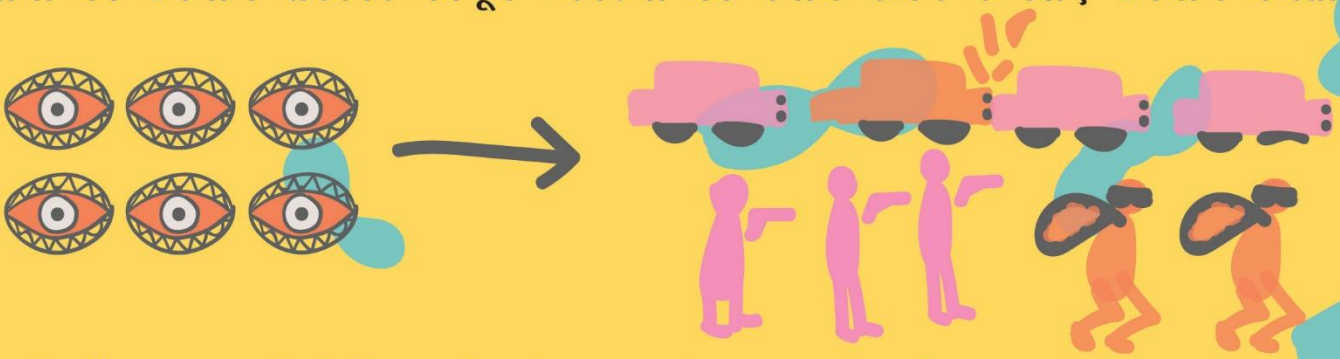
निगरानी

1. जरूरत से अधिक निगरानी आपकी आजादी खत्म कर सकती है.

2. सरकार और कंपनीयां का दायरा तय होना चाहिए कि निगरानी क्यों रखी जा रही है.

3. अधिक निगरानी, सूचनाओं का बहाव रोक सकती हैं.

4. निगरानी का उपयोग सरकारें कानून–व्यवस्था को बनाये रखने के लिए उपयोग करती हैं.



5. निगरानी के सवाल को निजिता से जोड़ कर देखा जाना चाहिए.

तो हमारी निजता का क्या?

क्या आपके फोन में सन्देश आते थे बैंक अकाउंट को आधार से जोड़ने के लिए. अगर हाँ तो, अब क्यूँ नहीं आता है, कभी सोचा है. दरअसल ऐसा करने से उच्चतम न्यायलय ने मना कर दिया था. मना क्यूँ किया था, क्यूँकी कोर्ट ने माना था कि निजता हमारा मौलिक अधिकार है. जिस चीज को निजी माना जाता है उसकी सीमाएँ और सामग्री संस्कृतियों और व्यक्तियों के बीच भिन्न होती हैं. निजता की सीमाएं आपके घरों में अलग हो सकती है.

समाज में अलग हो सकती है. सरकार को दी जाने वाली जानकारी में निजता की सीमाएं अलग हो सकती हैं. सोशल मीडिया में दी जाने जानकारियों में निजता अलग हो सकती है. सरकार ने शुरूआती दौर में, योजनाओं को लागू करने के लिए आधार के उपयोग की बात कही थी. फिर सरकार सिम कार्ड तक के लिये आधार कार्ड को अनिवार्य करने का प्रयास कर रही थी. बैंक के खाते को आधार से जोड़ने की बात कह रही थी. जैसे कि सन्देश आते रहते थे. जब आप आधार को बैंक अकाउंट से जोड़ते हैं तो सरकार आप पर निगरानी आसानी से रख सकती है. ठीक उसी प्रकार आपके बीमा से लेकर सिम कार्ड के द्वारा बहुत कुछ पर निगरानी रखी जा सकती है. यह सब आम जनता की शक्ति को कमजोर करेगी.

तो हमारी निजता का क्या?

1. आप कब क्या करते हैं, क्या खाते हैं, कौन सी दवा लेते हैं, कहाँ जाते हैं जैसी हर बात पर अगर कोई हर समय नजर रखने लगे तो आपकी प्रतिक्रिया क्या होगी?

2. निजता व्यक्तिगत इच्छाओं के सम्मान करने का हक देता है, यदि किसी व्यक्ति के पास कुछ निजी रखने की वाजिब इच्छा है, तो उसे निजी रखने का पूरा हक़ है.

3. निजता भारतीय संविधान में मौलिक अधिकार का हिस्सा है.

4. निजता का हनन हमारे सोचने–समझने की शक्ति को भी प्रभावित करेगा

5. हम किया राजनितिक गतिविधि करते हैं, किस राजनितिक पार्टी का समर्थन करते है जैसी जानकारियों का सम्मान नहीं किया और निजी रखी नहीं गयी तो लोकतंत्र खतरे में पड़ सकता है.

और ये निगरानी कैसे रखी जाती है?

तकनीक केवल अब साधन बनाने तक सीमित नहीं है, यह अब नयी प्रक्रिया को जन्म दे रही है जो पहले से कहीं अधिक शक्तिशाली है. आर्टिफीसियल इंटेलिजेंस (एआई) मानव बुद्धि के अनुकरण को मशीनों में संदर्भित करता है. मनुष्यों की तरह सोचने और उनके कार्यों की नकल करने के लिए उनको तैयार किया जाता है. आर्टिफीसियल इंटे. लिजेंस बिना जानकारियों के खिलौना मात्र है. बिना डेटा के मशीन को काम करना संभव नहीं है. आर्टिफीसियल इंटेलिजेंस उपयोग करके संसाधानों की बचत की जा सकती है.

एआई

ट्रैफिक से लेकर कृषि तक में इसका उपयोग किया जा सकता है. आत्महत्या से लेकर हिंसा तक को रोका जा सकता है. स्वास्थ्य सम्बन्धी जानकारियों का विश्लेषण करके ये तक पता किया जा सकता है कि कैसे व्यक्ति कि आत्महत्या करने की सम्भावना है. शिक्षा के क्षेत्र में उपयोग में कर ये पता किया जा सकता है कि कैसे छात्रध्छात्रों के विद्यालय छोड़ने की सम्भावना अधिक है. लेकिन तेजी से होते तकनीक के विकास के साथ इसके बेकाबू होने का खतरा उतना ही अधिक है. आर्टिफिशियल इंटेलिजेंस का उपयोग शिक्षा, स्वास्थ्य इत्त्यादि क्षेत्रो में किया जा रहा है. आर्टिफीसियल इंटेलिजेंस के उपयोग से नीतियों को बनाने में सहायता मिलेगी. इससे होने वाले के खतरे बारे में जागरूकता महत्वपूर्ण है.

और ये निगरानी कैसे रखी जाती है?

1. सार्वजानिक जगहों पर निगरानी सीसीटीवी कैमरे के जरिये रखी जाती है.

2. इन कैमरों से इकठ्ठा किये जा रहे डेटा का उपयोग कौन कर रहा है, किस लिए कर रहा है, कब कर रहा है जैसे सवाल महत्तवपूर्ण हैं.

3. सोशल मीडिया पर आर्टिफीसियल इंटेलिजेंस जैसी तकनीक का उपयोग करके रखी जाती है.

4. आर्टिफीसियल इंटेलिजेंस, बिना डेटा किसी काम की तकनीक नहीं है.

5. अपराध रोकने, अच्छी स्वस्थ्य सुविधाएँ जैसे कामों में आर्टिफीसियल इंटेलिजेंस अच्छे परिणाम दे सकते हैं, लेकिन इस सब में निजिता का सवाल पहले से कहीं अधिक महत्त्वपूर्ण हो जाता है.

तो आर्टिफीसियल इंटेलिजेंस से परेशानी क्या है?

भेदभावः

ऑनलाइन, ऑफलाइन, कंपनियां और सरकारें हमारे बारे में डेटा एकत्र करती हैं. वह यह निर्धारित करती हैं कि हम क्या विज्ञापन देखते हैं. सरकारें नीतियाँ तय करती हैं, जो कि बहुत प्रकार से हमारे जीवन में अवसरों को प्रभावित करती हैं. जिन विज्ञापनों को हम ऑनलाइन देखते हैं, या हमें नौकरी के साक्षात्कार के लिए आमंत्रित किया जाता है, या ये निर्णय लिया जाता है कि हम किसी योजनाध्नीतियों के लाभ लेने के योग्य हैं या नहीं, हमें ऋण मिलेगा के नहीं, हमारे फसलों का बिमा मिलेगा के नहीं, इसका फैसला अपारदर्शी प्रणालियों द्वारा किया जाता है, जो कि अत्यधिक महीन डेटा पर निर्भर करता है, तो आपको कैसा लगेगा?

डेटा के आधार पर लिया गया निर्णय, समाज में पहले से मौजूद असमानताओं और भेदभाव को सुगम बना सकता है. परिणामस्वरूप, समाज में डेटा के कारण होने वाले शोषण से, सबसे अधिक पहले से शोषित वर्ग को प्रभावित होगा. जो लोग इस धारा में नहीं आ सकेंगे उन्हें सरकारें भी भुला देंगी और इससे प्रभावित होने वालों में पंक्ति में खड़े आखिरी लोग जैसे, किसान, मजदूर, अल्पसंख्यक, अनुसूचित जनजाति से आने वाले अधिक होंगे.

तो आर्टिफीसियल इंटेलिजेंस से परेशानी क्या है?

पारदर्शिताः

आर्टिफिशियल इंटेलिजेंस की सफलता और घटनाक्रम में कई नई चुनौ. तियों और समस्याएं सामने आ रही हैं. जैसे–जैसे एआई एल्गोरिदम अधिक उन्नत होते जा रहे हैं, उनके आंतरिक कामकाज की समझ बनाना अधिक कठिन होता जा रहा है.

इसका एक कारण यह है कि उन्हें विकसित करने वाली कंपनियां अपने मालिकाना एल्गोरिदम की जांच की अनुमति नहीं देती हैं. हमें ये समझाने का प्रयास किया जा रहा है कि एआई अपनी बढ़ती जटिलता के कारण अपारदर्शी हो रहा है. यह एक नयी समस्या का रूप धारण कर सकता है क्यूंकि, आर्टिफिशियल इंटेलिजेंस हमारे जीवन का अभिन्न हिस्सा बनता जा रहा है.

तो आर्टिफीसियल इंटेलिजेंस से परेशानी क्या है?

1. आपको ऋण मिलेगा की नहीं, आपको किसी कॉलेज में दाखिला मिलेगा की नहीं, आपको नौकरी मिलेगी की नहीं अगर यह सब डेटा के आधार पर, अपारदर्शी ढंग से होने लगे आपकी प्रतिक्रिया क्या होगी?

2. आर्टिफीसियल इंटेलिजेंस के द्वारा लिए जाने वाले फैसलों में पारदर्शिता की कमी है, इस के कारण संदेह खड़े हो रहे हैं.

3. आर्टिफीसियल इंटेलिजेंस के कारण भेदभाव का भी खतरा बढ़ सकता है.

4. फेसिअल रिकग्निशन जैसी तकनीक का उपयोग करके आपकी हर गति. विधि पर नजर रखी जा सकती है, ऐसी तकनीकों का अगर सही उपयोग नहीं किया गया तो उत्पीड़िन की आशंका और प्रबल हो जाएँगी.

5. आपकी भावनाओं को समझ कर ऐसी तकनीकों का उपयोग करके आपका भावनात्मक शोषण किया जा सकता है, और अधिक भयावह यह है कि आपको एहसास तक नहीं होगा.

तो हल क्या है?

इन सारी समस्याओं से लड़ने के लिए सरकार डेटा प्रोटेक्शन का कानून बनाने जा रही है. जिसमें कहा जा रहा है कि व्यक्तिगत डेटा से संबंधित व्यक्तियों की गोपनीयता को सुरक्षा प्रदान की जाएगी. व्यक्तिगत डेटा के प्रवाह और उपयोग को निर्दिष्ट किया जायेगा.व्यक्तिगत डेटा को संसाधित करने वाले व्यक्तियों और संस्थाओं के बीच विश्वास बहाल करने का प्रयास किया जायेगा. नागरिकोंके मौलिक अधिकारों की रक्षा की जाएगी. डेटा के प्रसंस्करण में संगठनात्मक और तकनीकी उपायों के लिए एक ढांचा बनाया जायेगा. डेटा केसीमापार हस्तांतरण के नियम तय किये जायेंगे. व्यक्तिगत डेटा प्रोसेसिंग करने वाली संस्थ. ाओं की जवाबदेही तय की जाएगी.

अनधिकृत और हानिकारक प्रसंस्करण के लिए उपाय किया जायेगा, और डेटा सुरक्षा प्राधिकरण स्थापित किया जायेगा. लेकिन समस्या है कि सरकार अपने संस्थानों को इससे अलग रखने का प्रयास कर रही है. सरकार राष्टीय सुरक्षा के नाम पर किसी से जानकारी मांग सकती है और आपके पास कोई अधिकार नहीं होगा इनकार करने का. इससे डर का वातावरण बढेगा. सरकार का जरुरत से अधिक निगरानी रखने के कारण अविश्वास का माहौल बनेगा. डेटा सुरक्षा प्राधिकरण को कोई स्वंत्रता न देकर केंद्र सरकार का जानकारियों पर एकाधिकार स्थापित होगा. सरकार इस का उपयोग अपने लाभ के लिए कर सकती है. हमें एक मजबूत डेटा प्रोटेक्शन कानून की लड़ाई जारी रखनी होगी.

तो हल क्या है?

1. एक मजबूत कानून जिससे आप अपने डेटा के दुरूपयोग होने की चिंता से मुक्त रहें

2. निगरानी कौन और क्यों रख रहा है इस को ले कर पारदर्शिता हो.

3. डेटा कब और कौन उपयोग कर रहा है इस को लेकर पारदर्शिता हो.

4. निजता का सम्मान रखा जाये

5. सरकारी संस्थाएं भी इस कानून के अधीन आएं

तो फिलहाल कैसे अपने डेटा को सुरक्षित रखा जाये?

फेसबुक, ट्विटर, इंस्टाग्राम, टिकटोक और स्नैपचौट जैसी सोशल नेटवर्किंग साइट्स आज हमारे समाज में मनोरंजन से लेकर अपने व्यक्तिगत विचार और समाचार साझा करने का अड्डा बन गया है. ऐसे में कुछ पल रुक कर सोचने समझने कि आवश्यकता है कि हम जो गति. विधि कर रहे हैं वह कौन देख रहा है, उस जानकारी का उपयोग कौन और कैसे कर रहा है. ख़ास कर कैम्ब्रिज एनालिटिका प्रकरण के बाद हमें अपने सोशल नेटवर्किंग साइट्स के प्राइवेसी की सेटिंग पर ख़ास ध्यान देना चाहिए.

जब आप सोशल मीडिया पर जुड़ते ही आपसे अक्सर आपके घर, आप किस विद्यालय में पढ़ते थे, वहां किन–किन गतिविधियों में हिस्सा लेते थे, आप फिलहाल कहाँ कार्यरत हैं, पहले कहाँ काम करते थे या आप किस राजनितिक पार्टी या विचारधारा का समर्थन करते हैं, यह सभी जानकारी संग्रहीत और ट्रैक की जा सकती है. कई साइट्स आपके मित्रों की सूची, व्यक्तिगत प्राथमिकताओं और उनके उपयोग की शर्तों में और अधिक जानकारी की अनुमति शामिल कर सकती हैं. यह सभी जानकारियां हमें हो सकता है हानिरहित लगती हों, लेकिन इनका उपयोग बड़ी–बड़ी कंपनीयां विज्ञापन के लिए और राजनितिक पार्टीयां आपको चुनाव में प्रभावित करने के लिए उपयोग कर सकती हैं. तकनीकी होते इस दौर में हमें अपनी निजिता की रक्षा स्वयं करने का प्रयास करते रहना चाहिए. कुछ सुझाव आपके लिए हम लेकर आएं हैं जो आपके लिए उपयोगी साबित हो सकते हैं.

तो फिलहाल कैसे अपने डेटा को सुरक्षित रखा जाये?

1. हमें मालूम है की यह काम कठिन है लेकिन प्राइवेसी के टर्म्स एंड कंडीशन को पढ़ने का प्रयास करें।

2. कौनसी जानकारी आपसे साझा करने को कही जा रही है इसका ध्यान रखें

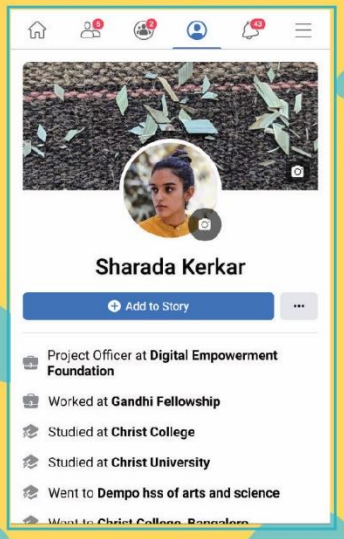
3. अपनी निजी जानकारी साझा करने से अधिक से अधिक बचने का प्रयास करें

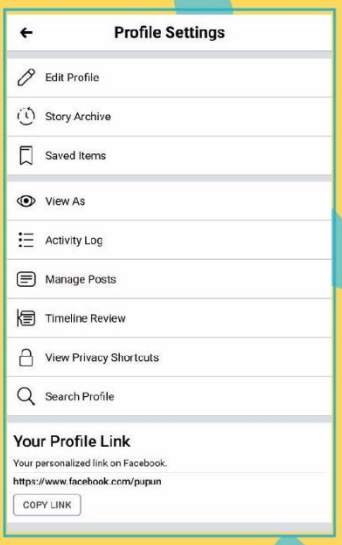
4. सोशल मीडिया पर फोटो, वीडियो, कोई जानकारी या कोई खबर सोच समझ कर साझा करें।

5. अपने फोन की प्राइवेसी सेटिंग का ध्यान रखें

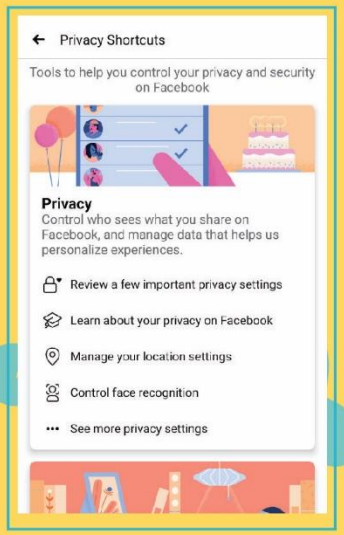
फेसबुक

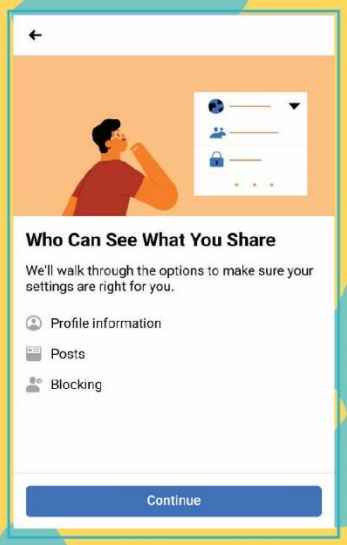
1. पहले तो यह तय करें कि आपकी जानकारी कौन देख सकता है, कौन नहीं. कुछ जानकारी जैसे, नाम, प्रोफाइल फोटो इत्यादि आप नहीं छुपा सकते, लेकिन कुछ जानकारी जैसे, आप अपनी गतिविधि, अपना पोस्ट, आप अपने मित्रों कि सूची इत्यादि छुपा सकते हैं. ऐसा करने के लिए फेसबुक प्रोफाइल पर दायीं ओर दिए गए तीन बिंदु वाले ऑप्शन पर क्लिक कर के सेटिंग में बदलाव करें.



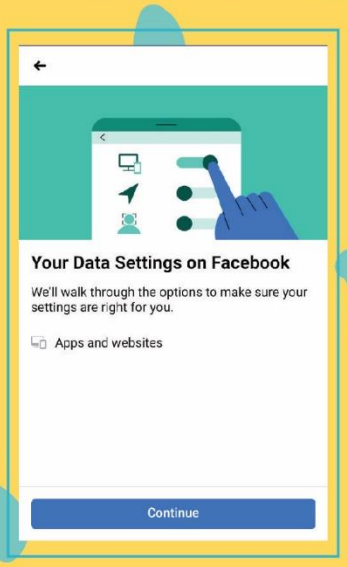


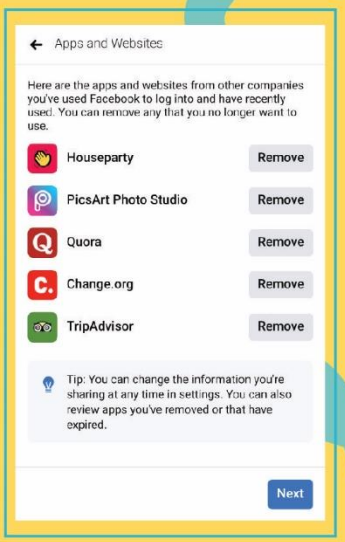
2. आपके द्वारा किये जाने वाले पोस्ट का ध्यान दें कि किस के साथ आप साझा कर रहे हैं. जब भी आप कुछ भी पोस्ट करने जाते हैं ऊपर दायीं ओर में एक ऑप्शन आता है जिस में फेसबुक आपको चुनने को कहता है कि किसके साथ साझा करना चाह रहे हैं, सिर्फ खुद तक, अपने मित्रों के साथ, या पब्लिक मतलब किसी के साथ भी साझा करना चाहते है.



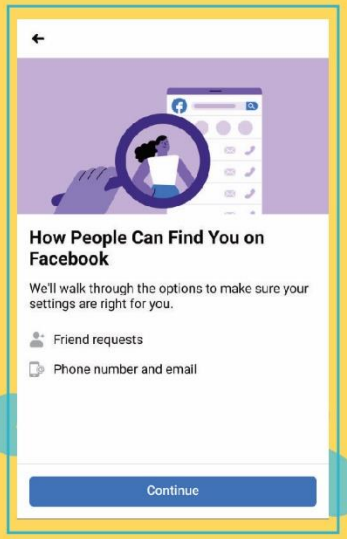


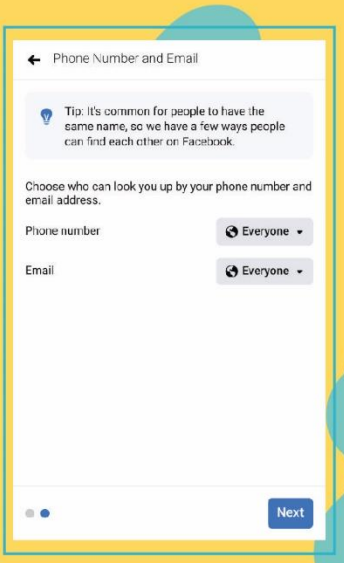
3. बिना अधिकार के दखल देने वाले एप्लीकेशन का ध्यान रखें, जब आप कोई नया एप्ल. ीकेशन डाउनलोड करते हैं तो, बहुत समय आपको वह एप्लीकेशन जल्दी से साइन अप करने के लिए आपको फेसबुक के माध्यम से, आपको लॉगइन करने को कहते हैं.ऐसे एप्ल. ीकेशन आपसे फेसबुक में की गयी गतिविधि पर नजर रख सकते है और आपके फेसबुक के डेटा का उपयोग भी कर सकते हैं. सेटिंग में जा कर आप एप्प्स पर क्लिक करके आप चुन भी सकते हैं की आप कौन सी सूचना उस एप्प के साथ साझा करना चाहते हैं.



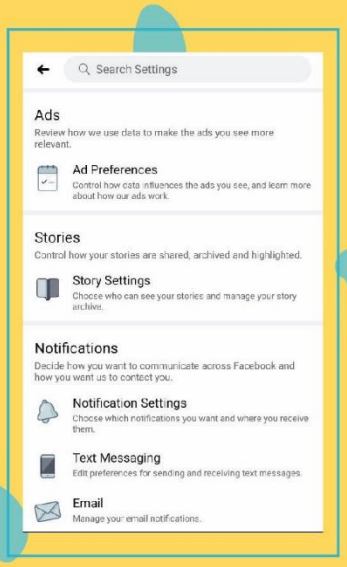


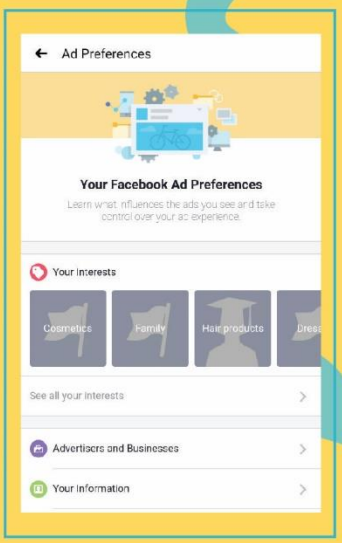
4. आपके फेसबुक प्रोफाइल को कौन ढूंढ सकता है इसका ध्यान रखें। आप सेटिंग्स में जा कर प्राइवेसी पर क्लिक करेंगे तो सर्च इंजन जैसे की गूगल पर सर्च करने से आपकी प्रोफाइल दिखेगे के नहीं का ऑप्शन आएगा, आप उसे नहीं करके अपनी प्रोफाइल को गूगल सर्च में आने से रोक सकते हैं.



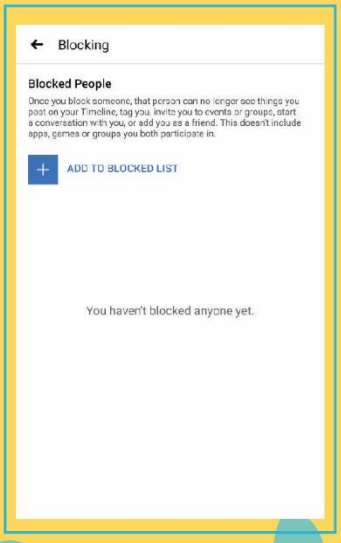


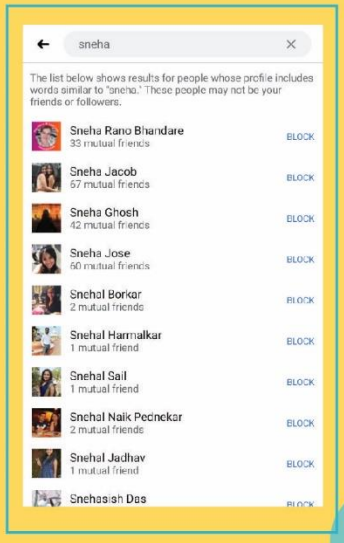
5. फेसबुक आपकी ब्राउजिंग गतिविधि को इंटरनेट पर ट्रैक करता है और इस डेटा का उपयोग आपको अधिक व्यक्तिगत विज्ञापन प्रदान करने के लिए करता है. यदि आपको यह अच्छा नहीं लगता है, तो आप फेसबुक को ऐसा करने से रोक सकते हैं. सेटिंग्स मेनू में, बाएं हाथ पर ''विज्ञापन'' पर क्लिक करें। पहला खंड फेसबुक, आपकी पसंद वाले विज्ञापन के बारे में कहता है. यदि आप इस सेटिंग को बंद कर देते हैं, तो आप अभी भी उतने ही विज्ञापन देख पाएंगे, लेकिन वे आपके वेब इतिहास से फेसबुक के अनुरूप नहीं होंगे।





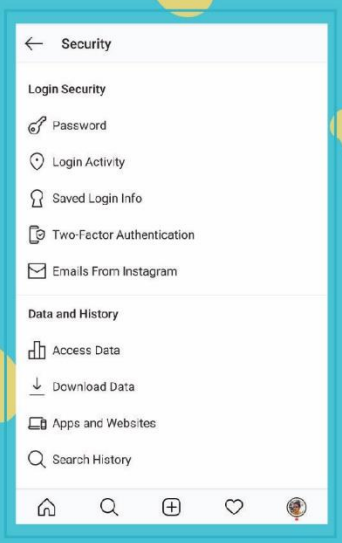
6. संदिग्ध उपयोगकर्ताओं को तुरंत ब्लॉक कर दें.

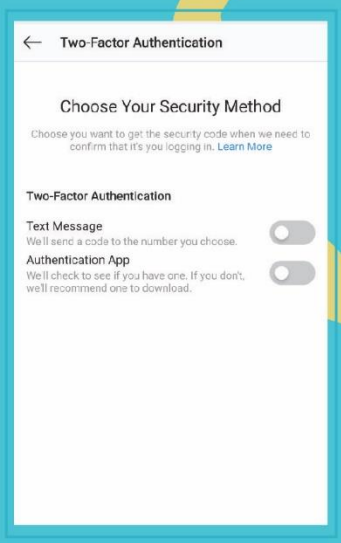




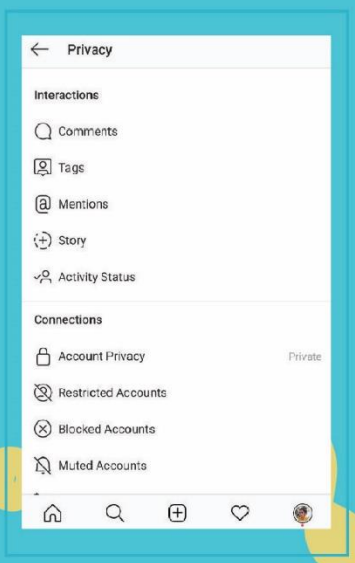
इंस्टाग्राम

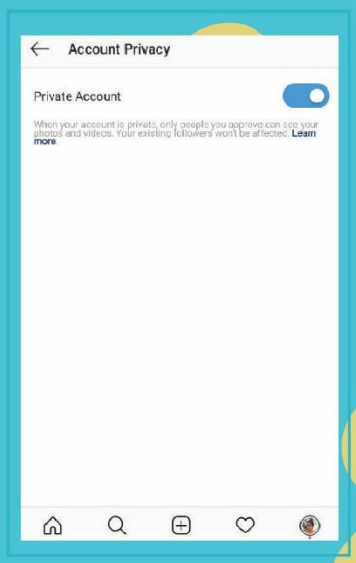
1. अपने अकाउंट को अधिक सुरक्षित रखने के लिए प्रोफाइल पर जायें, सेटिंगस पर क्लिक करें, सिक्योरिटी या सुरक्षा जो भी ऑप्शन आ रहा है उस पर क्लिक करें, टू फैक्टर ऑथेंटिकेशन को ऑन करके टेक्स्ट मैसेज वाले ऑप्शन को भी ऑन कर दें



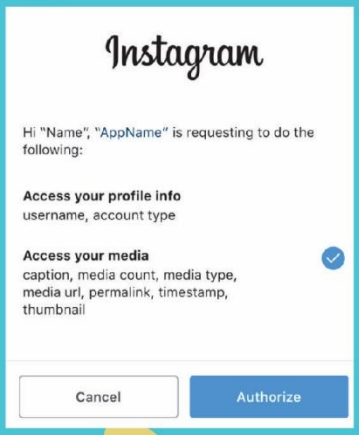


2. अपने अकाउंट को प्राइवेट रखें, प्राइवेट करने के लिए प्रोफाइल पर क्लिक करें, सेटिंग्स में जा कर प्राइवेसी में जाएँ और प्राइवेट अकाउंट को ऑन कर दें.

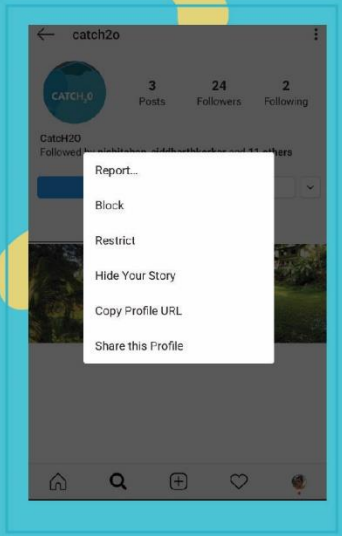




3. किसी थर्ड पार्टी एप्लीकेशन अगर आपसे इंस्टाग्राम की अनुमति मांगता है तो सावधानी से दें, यह देखें कि वह कौन सी जानकारियां मांग रहा है. आप सेटिंगस में जा कर ऑथो. राइज्ड अप्प पर क्लिक करके वापिस भी ले सकते हैं.

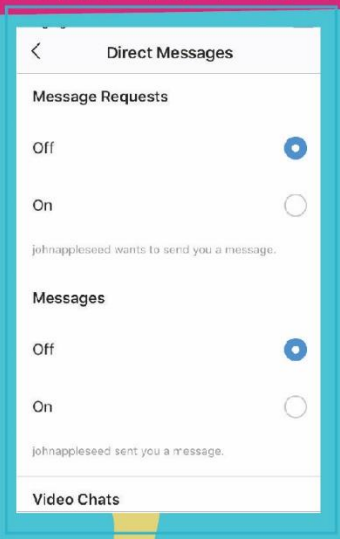


4. संदिग्ध उपयोगकर्ता को तुरंत ब्लॉक करें, किसी को ब्लॉक करने के लिए उसकी प्रोफाइल पर जाएँ, और तीन बिंदु वाले ऑप्शन पर क्लिक करें, ब्लॉक का ऑप्शन दिख जायेगा.



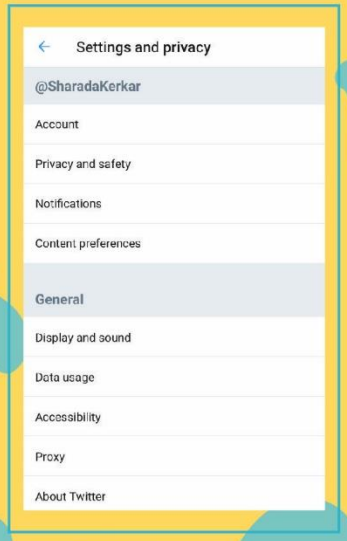
5. अपनी इंस्टाग्राम पर की गयी गतिविधि को छुपा कर रखें, ऐसा करने के लिए आप प्रोफाइल पर जा कर सेटिंग्स में जाएँ और एक्टिविटी स्टेटस को ऑफ कर दें.

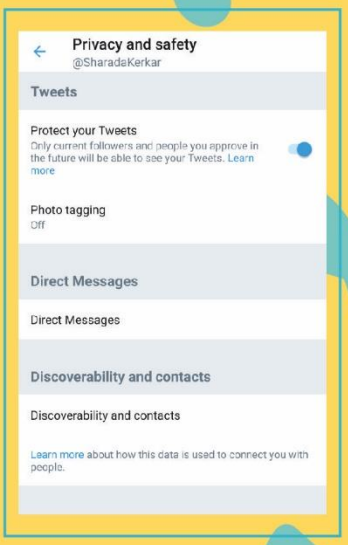
6. प्रत्यक्ष सन्देश भेजने वाली सुविधा को बंद करके रखें, ऐसा करने के लिए आप प्रोफाइल पर जा कर सेटिंग्स में जाएँ और डायरेक्ट मैसेज को ऑफ कर दें



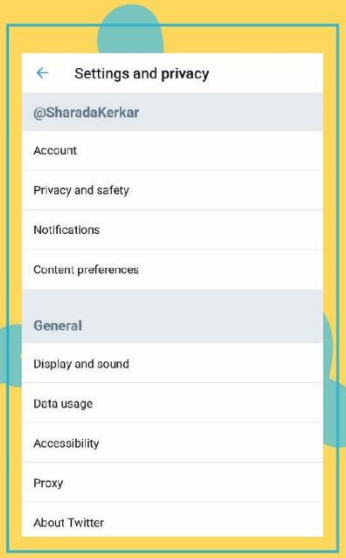
ट्विटर

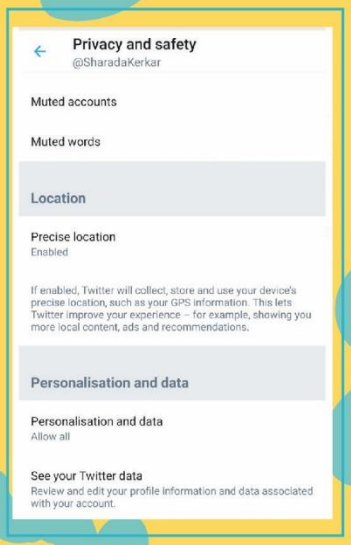
1. सबसे पहले अपने अकाउंट को प्राइवेट अवश्य करें, ऐसा करने के लिए प्रोफाइल पर क्लिक करें, सेटिंग में जा कर प्राइवेसी में जाएँ, फिर प्रोटेक्ट ट्वीट को ऑन कर दें. वहीं उस के निचे ट्वीट लोकेशन मतलब का ऑप्शन दिखेगा मतलब की आपने ट्वीट कहाँ से किया है, किस फोन से किया है इत्यादि उसको ऑफ कर दें.





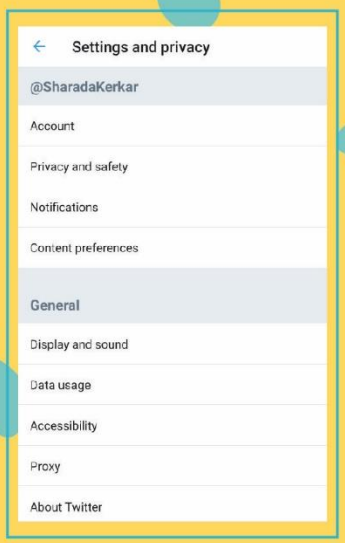
2. प्रोफाइल पर जाने के बाद सिक्योरिटी सेटिंगस के भीतर आपको ट्विटर यह नियंत्रित करने की अनुमति देता है कि ट्विटर आपकी कितनी जानकारी का उपयोग करेगा उदा. हरण के लिए, अधिकांश विकल्प काफी आत्म व्याख्यात्मक हैं – व्यक्तिगत विज्ञापन, या ट्विटर के व्यवसाय भागीदारों के साथ अपने डेटा को साझा करना इत्यादि।

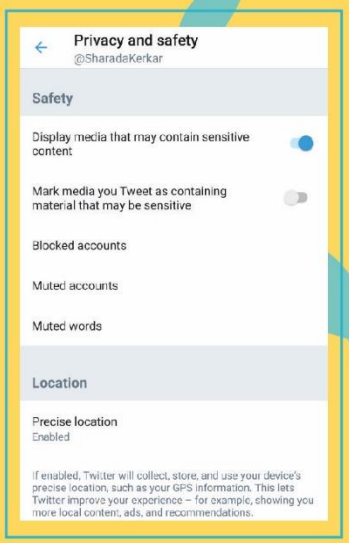




उस में एक ऑप्शन यह भी है की क्या ट्विटर एक डिवाइस से दूसरे को निजीकृत करने के लिए जो एकत्र करता है उसका उपयोग कर सकता है के नहीं, और यह ट्विटर एकीकरण के तीसरे पक्ष के साइटों से डेटा को शामिल करता है. यदि आप इस विकल्प को ऑन करते हैं, तो ट्विटर इस जानकारी का उपयोग आपको अन्य उपकरणों और साइटों पर आपके द्वारा की गई चीजों के आधार पर विज्ञापन देने के लिए कर सकता है.

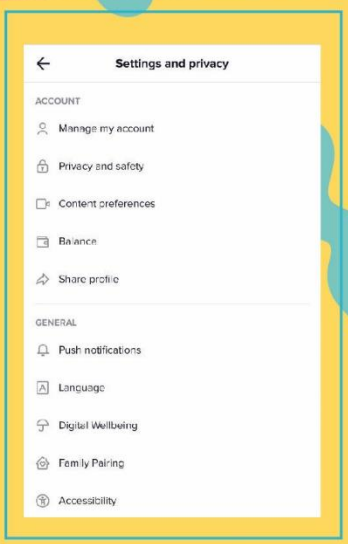
3. सेटिंगस में जा कर आप यह भी तय कर सकते हैं की आपको संवेदनशील पोस्ट देखने में रूचि है के नहीं.

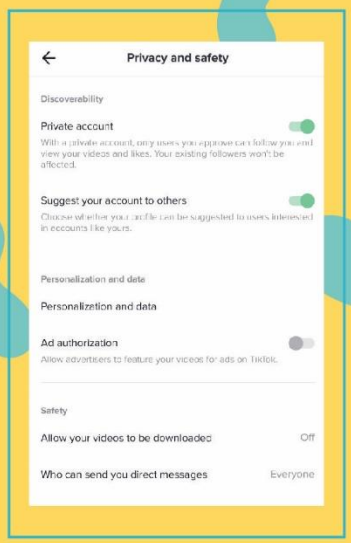




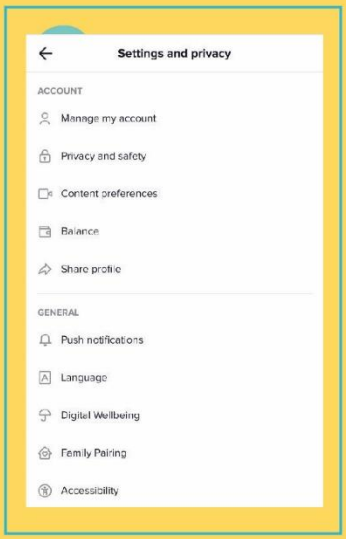
टिकटॉक

1. पहले अपने अकाउंट को प्राइवेट रखें, प्राइवेट रखने के लिए प्रोफाइल पर जायें और दायीं ओर तीन बिंदु वाले ऑप्शन पर क्लिक करें, प्राइवेसी और सेटिंग्स के ऑप्शन पर क्लिक करेंगे तो अकाउंट प्राइवेट करने का ऑप्शन आयेगा, उसे ऑफ कर दें.

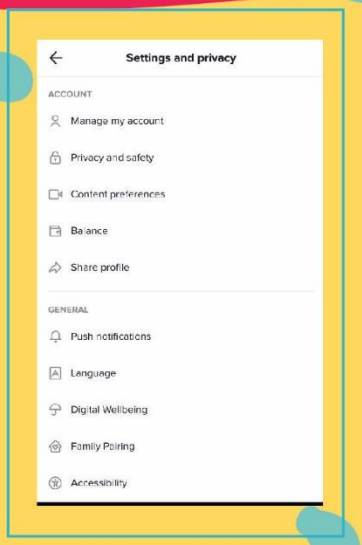


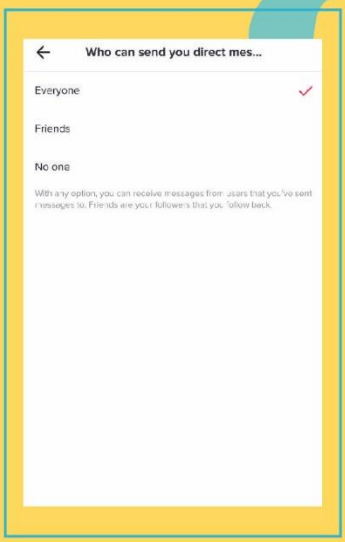


2. डिजिटल वेलबीइंग को ऑन करके आप यह तय कर सकते हैं के बच्चे कितने समय के लिए उपयोग कर सकते हैं और अनुचित सामग्री को ब्लॉक भी कर सकते है, ऐसा करने के लिए टिकटॉक एप्प की सेटिंग्स में जाएँ और डिजिटल वेल बीइंग को ऑन कर सकते हैं और पासवर्ड भी आप अपनी पसंद से लगा सकते हैं.

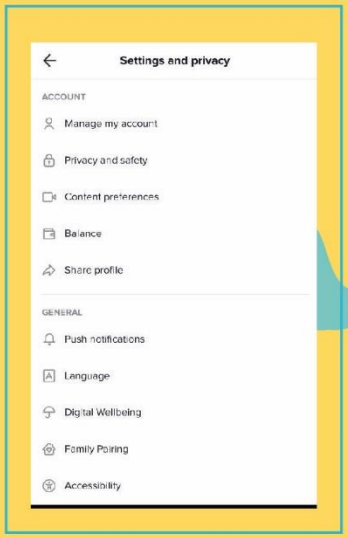


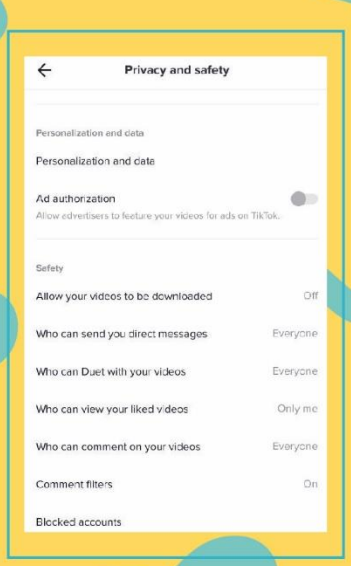
3. आप अपने एप्प की सेटिंग्स के प्राइवेसी एंड सेफ्टी वाले सेक्शन में जा कर कौन आपके पोस्ट को प्राइवेट कर सकता है, आपके मित्र या कोई भी का ऑप्शन चुन सकते हैं.



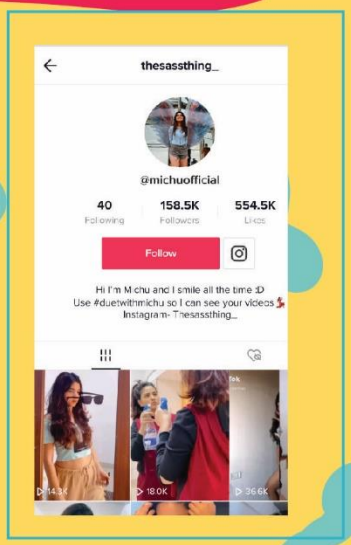


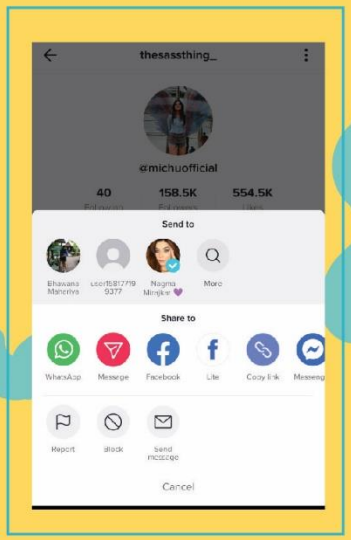
4. आपके किसके साथ युगलबंदी करना चाहते हैं, प्राइवेसी एंड सेफ्टी सेटिंग्स में जा कर यह भी तय कर सकते हैं, जैसे की किसे के साथ भी या सिर्फ आप जिसको जानते हैं उसके साथ.





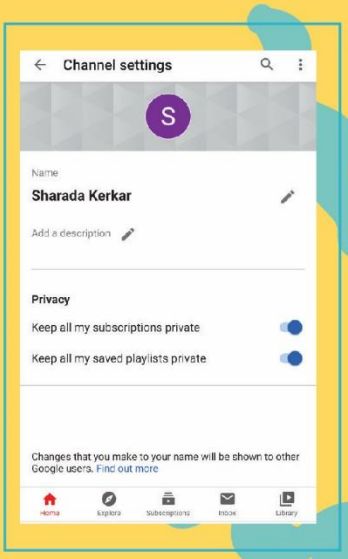
5. संदिग्ध उपयोगकर्ता को तुरंत ब्लॉक करें, ऐसा करने के लिए आपको जिन्हें ब्लॉक करना है उसके प्रोफाइल पर जाएँ और वहां आपको तीन बिंदु वाले ऑप्शन पर क्लिक करते ही ब्लॉक का ऑप्शन दिखेगा.

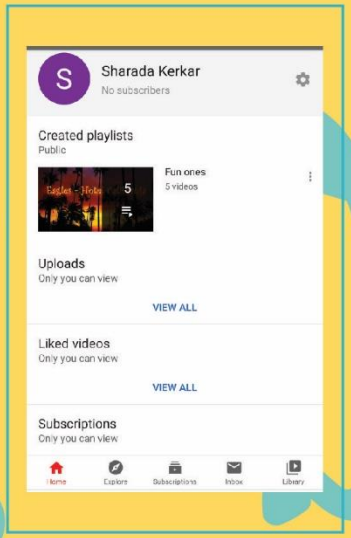




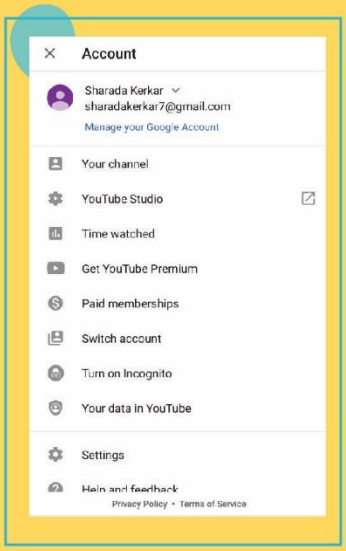
यूट्यूब

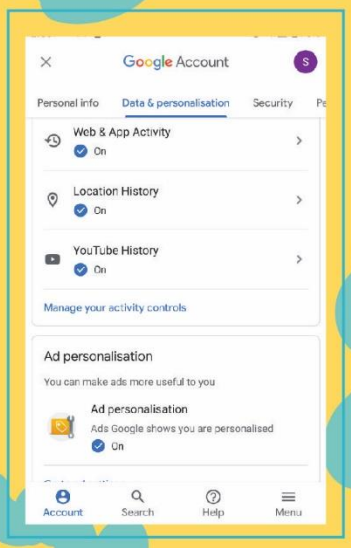
1. सबसे पहले आप क्या देखते हैं और क्या पसंद करते हैं उसे प्राइवेट रखें, ऐसे करने के लिए आपको यूट्यूब की सेटिंग्स के ऑप्शन में जाना होगा वहां आपको प्राइवेसी पर क्लिक करते ही आपको, आपके द्वारा पसंद किये गए, आपके द्वारा सेव किये गए वीडियो और आपके द्वारा सब्सक्राइब किये चौनल्स को गोपनीय रखने का ऑप्शन दिखेगा, उसके सामने आयतनुमा बॉक्स पर टिक कर दें.





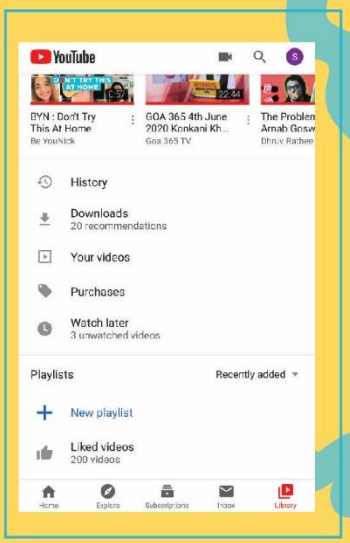
2. गूगल आपके द्वारा देखे जाने वाले यूट्यूब वीडियो पर नजर रखता है, और यह उस जानकारी का उपयोग वैयक्तिकृत विज्ञापन देने के लिए करता है. लेकिन यदि आप अपनी विज्ञापन की प्राथमिकताएं ट्रैक नहीं करना चाहते हैं, तो आप इसे बंद कर सकते हैं.

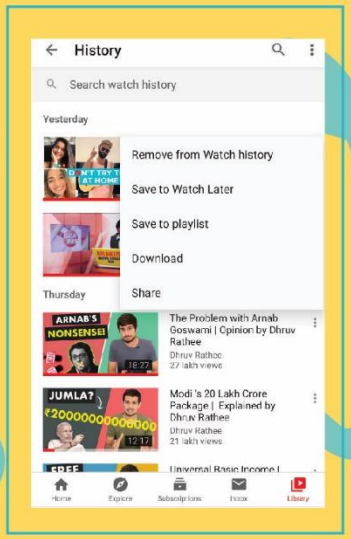




यदि आप वैयक्तिकृत विज्ञापनों का बुरा नहीं मानते हैं, लेकिन फिर भी अपनी गोपनीयता पर कुछ नियंत्रण चाहते हैं, तो आप गूगल द्वारा आपके हितों (उदाहरण के लिए, संगीत में आपके रुचि) के बारे में कुछ जानकारी हटा सकते हैं. ऐसा करने के लिए आपको अपने अकाउंट के प्राइवेसी सेटिंगस में जाना पड़ेगा, वहां आपकी रूचि पर आधारित विज्ञापन (।के ईंमक वद उल पदजमतमेज) का ऑप्शन दिखेगा आप वहां अपनी प्राथमिक. ताएं बदल सकते हैं.

3. आप, अपने द्वारा देखे हुए वीडियो को नियमित रूप से डिलीट करते रहा करें, यूट्यूब के दाएं ओर लाइब्रेरी पर क्लिक करते ही हिस्ट्री का ऑप्शन दिखेगा वहां आप जा किसी भी वीडियो के सामने तीन बिंदु वाले ऑप्शन पर क्लिक करके उस वीडियो को डिलीट कर सकते हैं.

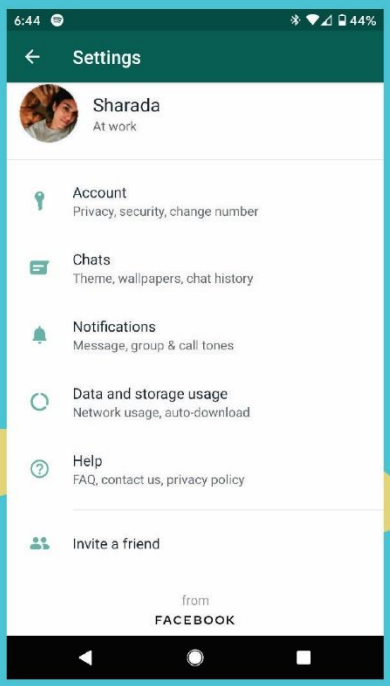


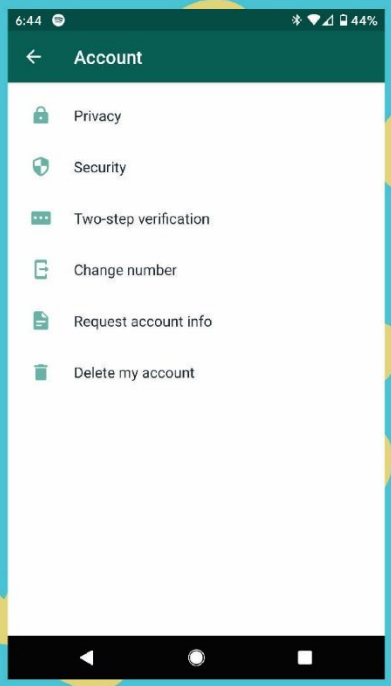


व्हाट्सप्प

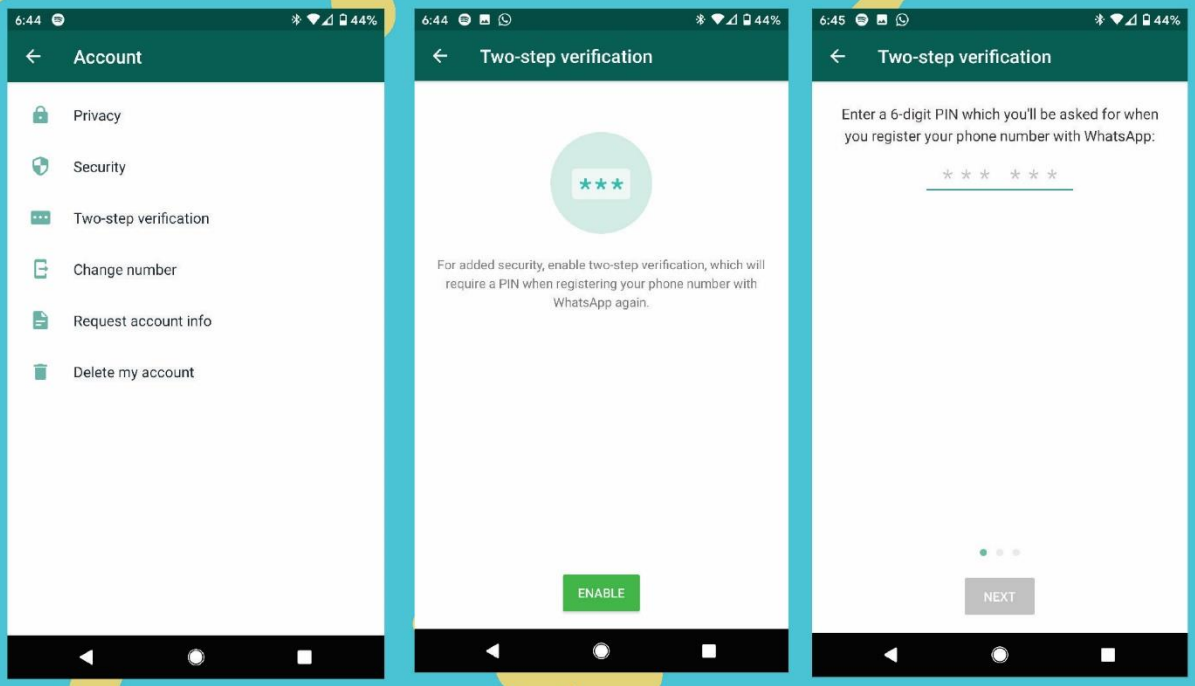
व्हाट्सएप सबसे तेजी से बढ़ते इंस्टेंट मैसेंजर में से है, और लगभग एक सोशल नेटवर्क की वेबसाइट की तरह हो चूका है. लेकिन अगर आप इसका उपयोग कर रहे हैं, तो कुछ ऐसे कदम हैं जो आपको अपनी सुरक्षा और गोपनीयता की रक्षा के लिए अपनाने चाहिए. व्हाट्सएप हालाँकि एंड–टू–एंड एन्क्रिप्शन के आधार पर कार्य करता है. यह डिफॉल्ट रूप से सक्षम है और इसे बंद नहीं किया जा सकता. एन्क्रिप्शन सुनिश्चित करता है कि आपके संदेश केवल प्राप्तकर्ता के फोन पर पढ़े जा सकते हैं. यह वॉयस कॉल और वीडियो कॉल के लिए समान है, दोनों ही एन्क्रिप्टेड होते हैं. ऐसे समय में जब निगरानी और निजता को लेकर संघर्ष चल रहा है, तो एन्क्रिप्शन ऑनलाइन गतिविधियों के लिए एक प्रकार का निजता प्रदान करता है.

1. जब कोई नया फोन या लैपटॉप किसी मौजूदा बात–चीत तक पहुँचता है, तो दोनों फोनों के लिए एक नया सुरक्षा कोड तैयार किया जाता है. और जब सुरक्षा कोड बदल जाता है तो व्हाट्सएप एक सूचना भेज सकता है. इस तरह, आप अपने मित्रों के साथ एक अलग मैसेंजर पर एन्क्रिप्शन की जांच कर सकते हैं, इसकी सुरक्षा सुनिश्चित कर सकते हैं. सुरक्षा सूचनाओं को चालू करने के लिए व्हाट्सप्प के सेटिंग पर जाएँ, अकाउंट पर क्लिक करें, सिक्योरिट में जा कर और जो बटन दिख रहा है उसे ऑन कर दें.



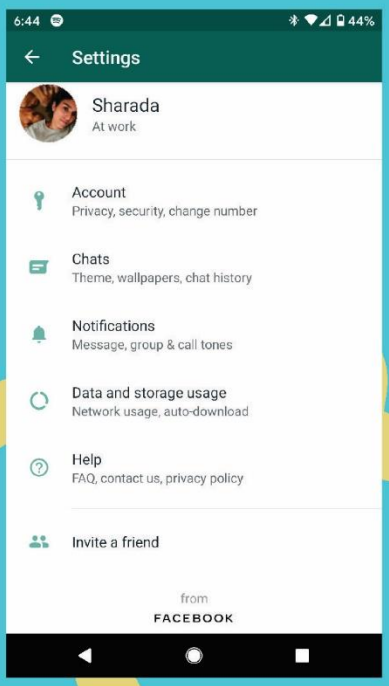


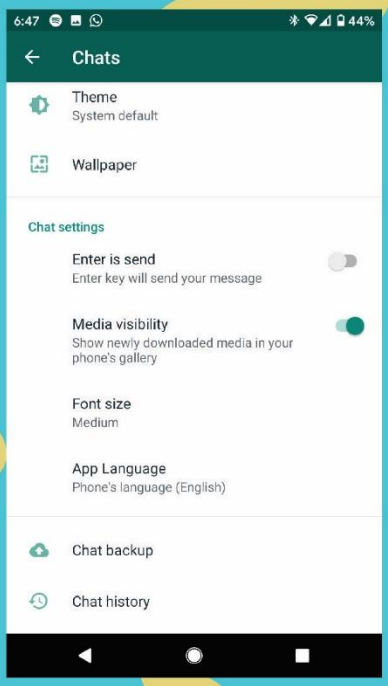
2. टू स्टेप वेरिफिकेशन को ऑन करें. इससे आपका डेटा अधिक सुरक्षित रह सकेगा टू स्टेप वेरिफिकेशन को सक्रिय करने के लिए, मेनू में जाएँ, सेटिंग्स पर क्लिक करें, अकाउंट पर क्लिक करें, टू स्टेप वेरिफिकेशन को इनेबल कर दें. छह अंकों का पिन कोड बनायें जिन्हें आसानी से याद रख सकते हैं. यदि आप इसे भूल जाते हैं तो उस कोड को पुनः प्राप्त करने के लिए अपना ईमेल पता जोड़ें.

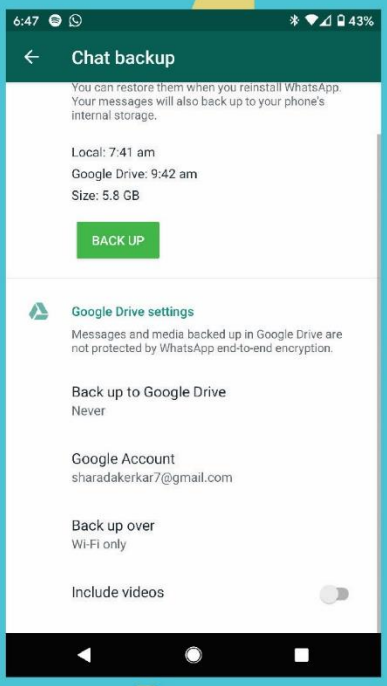


3. किसी भी प्रकार के संदेहपूर्ण लिंक पर क्लिक न करें. इससे आपके चौट के हैक होने के खतरे बढ़ जायेंगे.

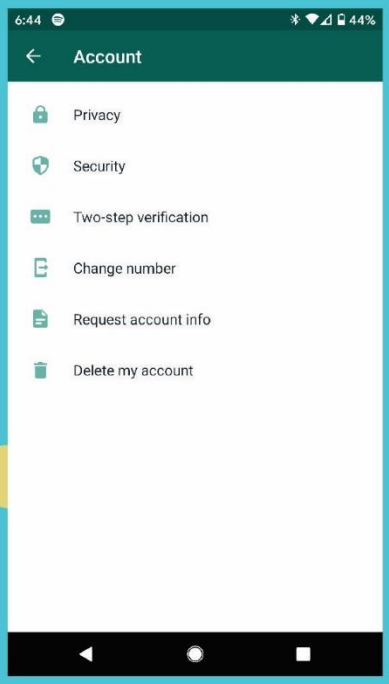
4. क्लाउड बैक अप को हमेशा बंद रखेंरू गूगल, एप्पल इत्यादि क्लाउड पर सेव किये गए डेटा से आपके ऊपर निगरानी रखना आसान हो जाता है. इसे बंद करने के लिए मेनू में जाएँ, सेटिंग्स पर क्लिक करें, चौट खोलें, चौट बैकअप पर जाएँ और गूगल ड्राइव पर बैकअप पर ष्नेवरष पर क्लिक कर दें.

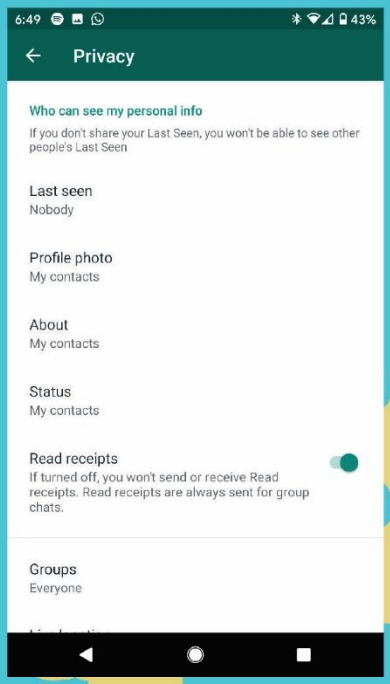




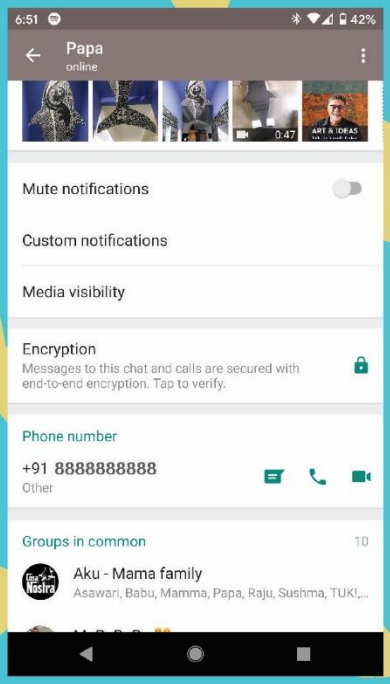


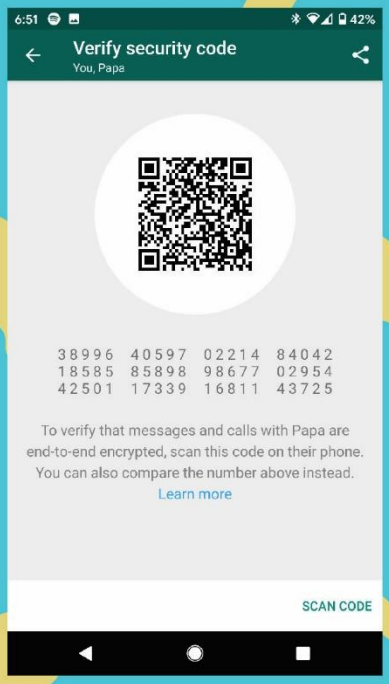
5. व्हाट्सएप सबसे निजी मेस्सेंजिंग एप्प नहीं है, लेकिन यह उपयोगकर्ताओं को कम से कम कुछ नियंत्रण देता है. सब कुछ अपने अनुसार है की नहीं देखने के लिये सेटिंग्स पर जाएँ, अकाउंट पर क्लिक करके प्राइवेसी पर जाएं. आप नियंत्रित कर सकते हैं कि आपका लास्ट सीन, प्रोफाइल फोटो, स्टेटस और लाइव लोकेशन कौन देख सकता है और कौन नहीं. आप यहां रीड रिसिप्ट को भी बंद कर सकते हैं, इससे नीले चेकमार्क बंद हो जाते हैं.





6. भले ही व्हाट्सएप डिफॉल्ट रूप से सभी चौट को एन्क्रिप्ट करता है, फिर भी कभी–कभी दोबारा चेक कर लेना बेहतर है. संवेदनशील जानकारी साझा करने से पहले ऐसा कर लेना चाहिए. एन्क्रिप्शन को सत्यापित करने के लिए, उस संपर्क के चौट विंडो में, संपर्क के नाम पर टैप करें और फिर एन्क्रिप्शन पर टैप करें. आपको एन्क्रिप्शन कोड दिखाई देगा. उसे स्कैन करके सत्यापित भी कर सकते हैं.





यदि मैं मोबाइल का उपयोग नहीं करता हूँ तो?

अगर आप लैपटॉप या कंप्यूटर के द्वारा इंटरनेट का उपयोग करते हैं ता ‘फायरफॉक्स (Firefox) सॉफ्टवेर का उपयोग कर सकते हैं. फायरफॉक्स ब्राउजर कि सेटिंग्स में प्राइवेसी पर क्लिक करें, आपको 'Tracking Protection in Private Windows' का ऑप्शन दिखाई देगा उसे डिफॉल्ट कर दें. इससे आपके द्वारा खोजी जा रही चीजें अधिक सुरक्षित रह सकेंगी.

'अधिकारों के बदलते स्वरूप: इंटरनेट, डेटा और निजता' को सामुदायिक स्तर पर जागरूकता पैदा करने के उद्देश्य से विकसित किया गया है. डेटा हमारे जीवन का महत्वपूर्ण हिस्सा बन चुका है इसलिए जरूरी है कि हम इसके उपयोग को बेहतर ढंग से समझने का प्रयास करें. डेटा का उपयोग कई सकारात्मक बदलावों के लिए किया जा रहा है. लेकिन इसके साथ आने वाले खतरे उससे कहीं अधिक गंभीर और चिंतित करने वाले हैं. इस लिए यह महत्वपूर्ण है कि हम इसके प्रभाव और इससे जुड़े अधिकारों को लेकर सतर्क रहें.

DEF
DIGITAL EMPOWERMENT foundation

Digital Empowerment Foundation
www.defindia.org