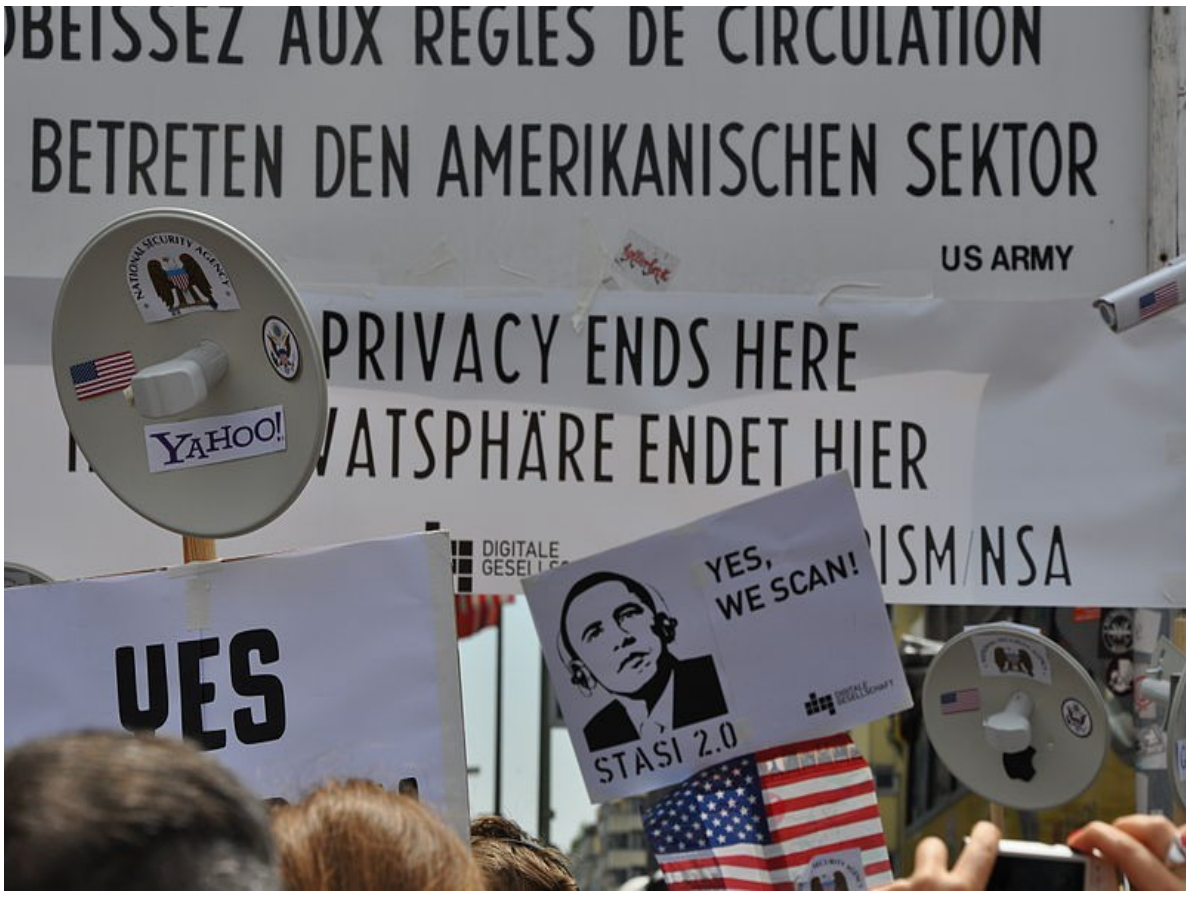
DIGITALE GESELLSCHAFT

DEMOTIPPS FÜR MOBILE GERÄTE UND SMARTPHONES



Eine Demo ist natürlich ein historisches Ereignis, das man festhalten möchte. Man will Infos, Fotos und Videos sofort mit Freunden oder auch der ganzen Welt teilen. Daher nehmen wir unsere mobilen Geräte mit und sehen uns dann mit dem Problem konfrontiert, dass wir auf eben jenen Geräten auch eine Menge private Daten gespeichert haben. Wir hoffen, dass wir euch mit dieser Anleitung einige Fragen beantworten und euch Tipps geben können, wie man seine Daten am besten sichert und welche Rechte ihr während der Demo habt, sollte es einmal brenzlig werden. Generell gilt natürlich: Seid kreativ, Humor ist stärker als Gewalt!

Seit einigen Jahren erfahren wir immer mehr, zu welchen Mitteln Sicherheitsbehörden greifen, um Kommunikationen von Demonstranten flächendeckend zu überwachen. Gleichzeitig sollte aber das Mithören unserer privaten Telefonate und die Durchsuchung unserer mobilen Geräte nicht ohne Anordnung möglich sein. Und es geht auch nicht nur um Inhalte: Schon die Tatsache, an einer bestimmten Demo teilgenommen zu haben, kann eine erhebliche Aussagekraft haben.

Niemand und kein Gerät ist jemals 100% sicher, aber es gibt ein paar Dinge, die ihr für die Sicherheit eurer persönlichen Daten tun könnt, bevor ihr auf die Straße geht. Dieser Leitfaden, der an einen Guide der EFF angelehnt ist, gibt euch einige gute Tipps.

VOR DER DEMO

Mach dir Gedanken darüber, welche Daten sich auf deinem Telefonen befinden. Zwar gibt es einige rechtliche Hürden, ehe jemand dein Handy beschlagnahmen und durchsuchen darf, doch ist es alles andere als sicher, dass euch das im Ernstfall wirklich hilft.

Und auch wenn niemand euer Gerät in die Hände bekommt, drohen durchaus Gefahren für die Privatsphäre. Denn seit 2012 ist bekannt, dass die Polizei flächendeckende Funkzellenabfragen während Demos durchführt.

Bei einer Funkzellenabfrage werden alle Verbindungsdaten ausgewertet, die in einer bestimmten, räumlich bezeichneten Funkzelle in einem bestimmten Zeitraum angefallen ist. Die Berliner Polizei hat beispielsweise im letzten Jahr auf diese Weise 50 Millionen Verkehrsdatensätze gesammelt. Damit lässt sich quasi ein elektronisches Register

anlegen, wer an welcher Demo teilgenommen hat - und zwar auch ohne dass es den geringsten Verdacht gegen die Personen gäbe, die so ins Raster der Behörden geraten.

Gegen die Funkzellenabfrage ist leider kaum ein Kraut gewachsen, sofern man das Handy nicht in den Flugzeug-Modus stellen will. Aber was die Inhalte des Handys angeht haben wir eine Reihe von Empfehlungen:

Schütze deine Daten!

Wenn du noch irgendwo ein älteres Handy hast, ist es empfehlenswert, dein jetziges vorübergehend zu ersetzen. So kannst du für den Fall der Fälle sicher gehen, dass deine Fotos, dein Adressbuch und andere Daten sicher zu Hause liegen.

Mach ein Back-up. Eine weitere und einfache Möglichkeit ist es, vor der Demo ein Back-up aller Inhalte, deines Adressbuchs und aller Nachrichten zu machen, um dann dein Gerät komplett löschen zu können. Dieses leere Gerät kannst du dann problemlos mit zur Demo nehmen. Nach der Demo holst du dir einfach alles mit dem Back-up zu Hause zurück. Wenn du allerdings meinst, dass du gar kein Handy brauchst, bringe einfach keins mit.

Sperre dein Handy mit einem Passwort. Der Passwortschutz kann dein Handy vor physischen Durchsuchungen schützen - aber vergiss nicht, dass er von Geheimdiensten oder anderen Behörden eventuell umgangen werden kann. Eine Kombination aus Zahlen und Buchstaben ist generell sicherer, denn eine Zahlenkombination lässt sich in wenigen Minuten knacken.

Benutze verschlüsselte Kommunikationswege. SMS können generell von deinem Anbieter gespeichert und mitgelesen werden - oder auch mit Hilfe von diversem Überwachungsmaterial, das in der Nähe der Demo aufgestellt wird (Stichwort IMSI-Catcher). Du solltest dich mit deinen Freunden vor der Demo mit verschiedenen Verschlüsselungstechniken und -diensten vertraut machen, um deine Nachrichten vor fremdem Zugriff zu schützen. Direkte Nachrichten über soziale Netzwerke können beim Senden teilweise verschlüsselt werden. Strafverfolgungsbehörden haben aber die Möglichkeit, mit Hilfe von Anordnungen die Herausgabe der Daten bei den Unternehmen anzufordern.

Zum Glück kann man alle Nachrichten und SMS durch den sogenannte Ende-zu-Ende-Verschlüsselung besser schützen. Mit Apps wie TextSecure (Whisper Systems) kannst du deine SMS und mit ChatSecure (Guardian Project) dein Instant-Messaging verschlüsseln. Auch die mobile Version von Cryptocat ist ganz gut für verschlüsselte Chats.In Deutschland relativ verbreitet ist außerdem die (kostenpflichtige) App Threema. Leider ist die Software nicht OpenSource, aber sicherlich doch etwas sicherer als offene Kommunikation über Facebook oder SMS.

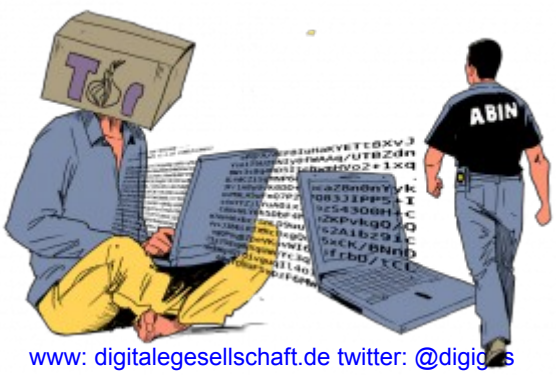
Wichtig: *Ende-zu-Ende-Verschlüsselung schützt nicht deine Metadaten.* Mit anderen Worten: Selbst wenn du alles verschlüsselst, können Behörden je nach System evtl. weiterhin sehen, mit wem du wann und wie lange telefonierst oder Nachrichten austauschst.

Behalte die Kontrolle über dein Telefon. Es ist empfehlenswert, dein Handy immer bei dir zu tragen und es nur dann einer Person deines Vertrauens in die Hand zu geben, wenn du meinst, dass dir eine Verhaftung bevorsteht. In jedem Fall solltest du dein Handy so einstellen, dass sich der Bildschirm sehr schnell automatisch sperrt. Übrigens: Es gibt keine rechtliche Verpflichtung, irgendwelchen Beamten seine Passwörter zu verraten. Das sollte man daher auch nicht tun, es sei denn nach Rücksprache mit rechtlichem Beistand.

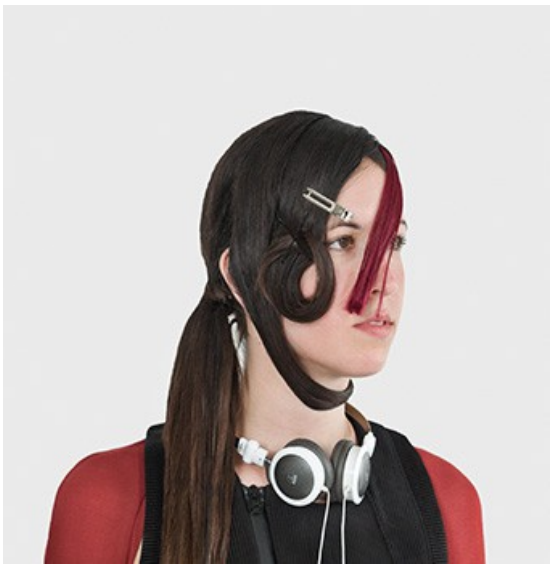
Mache Bilder und Videos von der Demo. Wir haben alle das Recht darauf, alles aufzunehmen, was sich vor unseren Augen im öffentlichen Raum abspielt. Obwohl die Polizei das nicht so gerne sieht und sich hin und wieder dagegen wehrt, meint das Bundesverfassungsgericht, dass "Dokumentationen von Polizeieinsätzen im öffentlichen Interesse" liegen. Lest Euch aber zur Sicherheit vor der Demo die Infos hier der Gruppe "BürgerInnen beobachten Polizei und Justiz" auch noch einmal genau durch.

Außerdem könnte man erwägen, Dienste zu nutzen, die das gesammelte Material direkt auf einen Server hochladen. Streamingdienste und sogar soziale Netzwerke sind praktisch, um zu verhindern, dass Beamte sie von den Geräten löschen können.

Nutzt Tor oder VPNs. Wenn ihr etwas im Netz nachschauen und surfen wollt, könnt ihr dies anonym über das Tor-Netzwerk tun. Für Android und iOS gibt es beispielsweise Orbot und Orweb. Eine weitere Alternative ist die Nutzung von bezahlten VPN-Diensten (die den Zugriff auf das Internet durch Tunnel ermöglichen), die zwar schneller als das Tor-Netzwerk sind, aber weniger gut eure Identität schützen.



Schminkt euch! Es gibt überall Kameras, die alle DemoteilnehmerInnen die ganze Zeit filmen. Ohne es zu wissen, kann dein Bild also schnell in einer Datenbank landen. Zum Glück haben schon mehrere Künstler nette Looks entworfen, mit denen man Gesichtserkennungssoftware entgehen kann. Hier ein wenig Inspiration:



Passt aufeinander auf! Dazu gehört auch, dass man die Privatsphäre aller MitdemonstrantInnen respektiert. Bevor du also Fotos über soziale Medien teilst, solltest du vorher soweit es geht das Einverständnis der Fotografierten einholen oder aber direkt dafür sorgen, dass die Personen nicht erkannt werden können. Mit der App ObscuraCam (Guardian Project) kann man zum Beispiel sehr einfach Gesichter verpixeln.

Hilfe, ich werde verhaftet!

Du hast das Recht zu schweigen - Das betrifft auch Informationen zu deinem Telefon. Bleibe immer ruhig und freundlich. Auf Verlangen sollte man sich zwar mit einem Personalausweis ausweisen und Angaben zur Person machen können - darüber hinaus darf man sich aber gegen jede weitere Mitarbeit sträuben. Du kannst eine Durchsuchung höflich verweigern und erklären, alle weiteren Fragen nicht ohne die Gegenwart eines Anwalts zu beantworten. Wenn ein Polizeibeamter dein Telefon sehen möchte, sag ihm freundlich und bestimmt, dass du einer Durchsuchung deines Geräts nicht zustimmst. Sollte der oder die Beamte nach deinem Passwort fragen, verweigere die Auskunft und fordere einen Anwalt. Jede Verhaftung verläuft anders und du solltest dich von einen Anwalt beraten lassen, damit du in dieser speziellen Situation Unterstützung bekommst.

Bitte beachte, dass die Polizei dich vielleicht nicht zur Herausgabe deiner Passwörter überreden kann - sie kann aber alles dafür tun, um dich unter Druck zu setzen. Sie können dich zeitweise festhalten, wenn du die Kooperation verweigerst. Du hast aber das Recht, spätestens am folgenden Tag einem Richter vorgeführt zu werden. Einfach wegsperren können sie dich also nicht.

Oft werden bei Demonstrationen auch Nummern von Anwälten, die während der Demo angerufen werden können, verteilt. Zudem steht oft eine **"EA-Nummer"** zur Verfügung, die ihre anrufen solltet, wenn ihr seht, dass ein Freund von euch verhaftet wird. Die Leute kümmern sich dann um alles weitere und versuchen, die betroffene Person schnellstmöglich wieder frei zu bekommen.

Die Berliner Strafverteidiger haben außerdem eine **Notfall-Hotline: 0172 - 325 55 53**. Diese Nr. sollte man sich merken oder einfach auf den Arm oder Hand schreiben und dann im Falle einer Verhaftung verlangen, dass dort angerufen wird (und nicht irgendwo).