Smartphone-Tracking

Wie Daten von kommerziellen Apps an den Staat gelangen

Cryptoparty Graz, 7.12.2020

Martin Gundersen (norwegischer Journalist):

Recherche, wie seine Daten von genutzten Smartphone-Apps über Umwege in die Hände eines Datenbrokers kamen, der mit US-Polizeibehörden zusammenarbeitet.

Februar 2020:

- 160 Apps auf ein zusätzliches Smartphone installiert
- dieses Gerät seitdem immer bei sich gehabt

Kommerzielle Überwachung:
begründet ihre vermeintliche Harmlosigkeit immer damit, dass

- die Daten doch nur für Werbung,
- ein besseres Nutzer:innenerlebnis oder
- ein bisschen Analyse verwendet würden.

- Schon durch vergangene Recherchen kam heraus, dass US-Behörden und das Militär gezielt kommerzielle Nutzerdaten aufkaufen und benutzen.
- Die US-Grenzbehörden haben aufgrund solcher gekauften Daten auch schon mal einen Drogenschmuggler geschnappt.

- Beteiligt an diesem Datenverkauf war auch das Unternehmen Venntel.

- Venntel war aus früheren Recherchen des "Wall Street Journal" und von "Vice" bekannt
- Venntel gehört zu den größten Sammlern von Standortdaten

Bei Unternehmen Venntel:

Ende August 2020 auf Grundlage der Datenschutzgrundverordnung (DSGVO) seine eigenen Daten angefragt.

Das Unternehmen ist nach der DSGVO verpflichtet, Auskunft darüber zu geben und jede:r Europäer:in hat das Recht diese Daten anzufragen.

„Fast einen Monat später erhielt ich einen interessanten E-Mail-Anhang von Venntel.

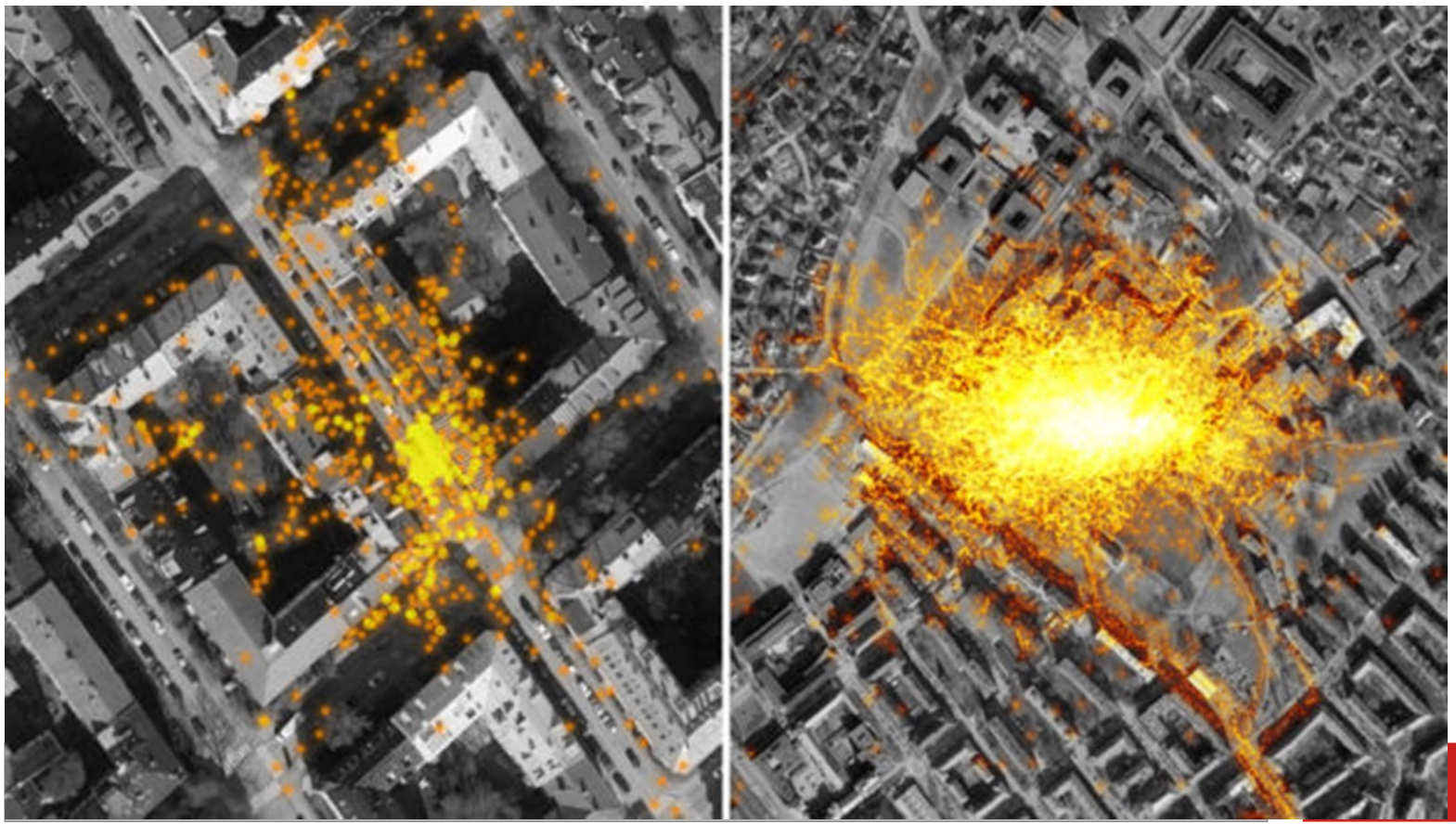
Er enthielt Informationen darüber, wo ich seit dem 15. Februar 75.406 Mal gewesen war.

Plötzlich konnte ich jeden meiner Schritte zurückverfolgen :

- auf einer Wanderung,
- auf einen Drink und
- bei einem Besuch bei meiner Großmutter in Südnorwegen.“

Urlaubswanderung

Wohn- und Arbeitsort



Obwohl kein Name und keine Telefonnummer in den Daten war, sei es einfach herauszufinden, wem die Daten gehören.

Deutlich und klar: Wohn- und Arbeitsadresse Gundersens erkennbar

Venntel informierte Gundersen darüber, dass seine Daten an Kunden des Unternehmens weitergegeben worden seien.

An welche Kunden, das verriet Venntel jedoch nicht...

Doch wie kamen die Daten überhaupt an Venntel?

In keiner der 160 Apps stand der Name Venntel, nicht einmal im Kleingedruckten, berichtet Gundersen.

Heraus bekam er aber, dass Venntel, die Informationen von seiner Mutterfirma, dem Datenbroker Gravy Analytics erhalten hatte.

Gravy Analytics wollte oder konnte die Herkunft eines Großteils der Daten gegenüber Gundersen auch nicht erklären.

Aber es tauchten die Namen der Firmen Predicio aus Frankreich und Complementics aus den USA auf.

In weiteren Anfragen kam heraus, dass ein großer Teil der ortsbezogenen Daten von einem slowakischen Unternehmen namens Sygic stammte, welches ein Portfolio von 70 Apps anbietet. Manche dieser Apps haben über 200 Millionen Nutzer.

Data flow from apps to Venntel

NRKbeta / Martin Gundersen

Gundersen hatte im Februar zwei Navigations-Apps von Sygic installiert, die beim Installationsprozess eine Einwilligung zur Personalisierung der Werbung erfordert hätten.

Am Ende landeten die Daten aber bei Gravy Analytics, das in ihren Geschäftsbedingungen schreibt, dass sie Daten für die Strafverfolgung und Nationale Sicherheit weitergeben.

Gundersen fragte drei auf Datenschutz spezialisierte Anwält:innen, alle drei hielten die Verwendung der Daten für einen Bruch der DSGVO.

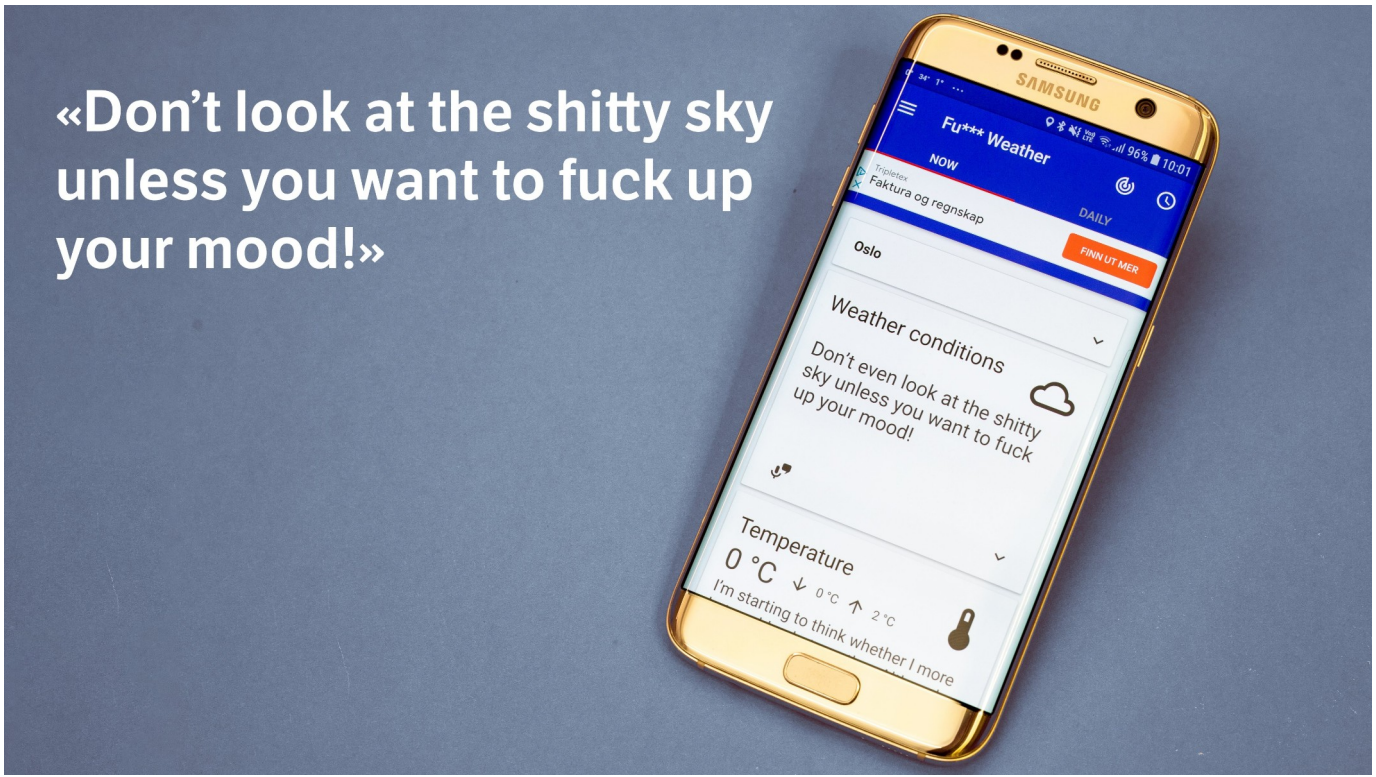
Doch nicht nur die Apps von Sygic lieferten die Daten bis zu Venntel, sondern auch die App Funny Weather.

Bei deren Installation stimmte Gundersen „Analytics“ und „Monetisation“ zu.

- https://funnyweather.zsuiwal.com/eula/
- https://funnyweather.zsuiwal.com/privacy/

„*The Application may collect the data even when it’s closed and/or not in use.*“

Auch hier fanden die befragten Anwälte eine Verletzung der DSGVO, da „Monetarisierung“ ein viel zu weit gefasster Verwendungszweck sei.


«Don’t look at the shitty sky unless you want to fuck up your mood!»
SAMSUNG
Fu*** Weather
NOW
DAILY
Faktura og regnskap
FINN UT MER
Oslo
Weather conditions
Don’t even look at the shitty sky unless you want to fuck up your mood!
Temperature
0 °C
I’m starting to think whether I more

Hinter Funny Weather steht keine große Firma.

Gundersen konfrontierte den Entwickler Lawiusz Fras mit den Daten bei Venntel.

Fras kannte zwar Venntel nicht, aber betonte, dass bei der App klar sei, dass manche Daten genutzt würden, um Geld zu verdienen.

Gundersen geht davon aus, dass die Daten über das französische Unternehmen Predicio zu Venntel gelangten.

Wolfie Christl,
österreichischer Daten- und Überwachungsforscher

https://crackedlabs.org

https://twitter.com/WolfieChristl

https://twitter.com/WolfieChristl

Ein norwegischer Journalist hat herausgefunden, über welche Smartphone-Apps und EU-Zwischenhändler 75.406 Datensätze über seinen Standort bei einer US-Firma gelandet sind, die personenbezogene Marketing-Tracking-Daten an US-Sicherheitsbehörden verkauft

Im Februar 2020 wurde erstmals klar, dass das, was viele schon lange befürchtet haben, wirklich passiert:

US-Sicherheitsbehörden, FBI, Homeland Security und Militär kaufen global über undurchsichtige Wege Standortdaten ein, die aus stinknormalen Apps von Wetter bis Navi stammen.

@martingund hat nun die Datenflüsse von zwei Apps bis zur Firma Venntel nachvollzogen, zu der in den letzten Monaten immer mehr Informationen aufgetaucht sind und die Verträge mit allen möglichen US-Behörden hat.

https://twitter.com/WolfieChristl

Zu den Zwischenhändlern gehört die französische Firma Predicio.

Laut einem sehr detaillierten Eintrag in einer Art von Datenhandels-Branchenverzeichnis verkauft Predicio Standortdaten von 61,5 Millionen "täglich aktiven" App-NutzerInnen, inklusive GPS-Koordinaten und personenbezogener ID, unter anderem aus Deutschland:

https://datarade.ai/data-products/raw-location-data-5013835a-b019-4d27-9ab2-42d6b5094687

https://twitter.com/WolfieChristl

Venntel bestreitet, die 75.406 norwegischen Datensätze an US-Behörden verkauft zu haben.

Und es bleibt unklar, welche anderen Daten über Predicio bei Venntel gelandet sind.

Aber unabhängig davon, ich sag mal, das was Predicio und Apps machen, geht sich mit DSGVO keinesfalls aus.

https://twitter.com/WolfieChristl

Es ist ein Paradigmenwechsel.

Anstatt - wie von Snowden 2013 aufgedeckt - mit hohem Aufwand den gesamten Internet-Datenverkehr abzusaugen, wird einfach die Infrastruktur der Werbe/Marketing/App-Datenmärkte für staatliche Überwachung genutzt.

Die Digitalwirtschaft ist kaputt.

In seiner Recherche kann Gundersen mit den Daten von Venntel heute nachvollziehen, wo er im Sommer wanderte und auf welcher Holzbank er wie lange eine Pause machte.

Genauso können das alle, die diese Daten kaufen und weiterverarbeiten.

Sie können sehen,

- wer in welche Arztpraxis geht,
- wer bei welchem Konzert ist und
- wo sich ein unvorsichtiger Journalist mit einem Informanten getroffen hat.

Dass staatliche Player diese Informationen nun einfach kaufen macht klar:

Kommerzielle Überwachung und staatliche Überwachung sind keine zwei getrennt zu denkenden Formen, sondern in Kombination noch viel verletzender für die Privatsphäre der Nutzer:innen als die einzelnen Formen für sich.

Für die staatlichen Player eröffnen sich völlig neue Möglichkeiten, an Daten heranzukommen:

Sie kaufen sie einfach auf dem unüberschaubaren Markt der Datenbroker anstatt mühsam mit klassischen Überwachungsinstrumenten selbst an sie zu gelangen.

Das FBI, die US-Grenzschutzbehörde CBP und die US-Immigrationspolizei ICE haben Verträge mit Venntel.

Venntel sagte gegenüber Gundersen, dass sie seine Daten nicht an ICE oder CBP weitergegeben hätten.

ICE und CBP antworteten Gundersen nicht auf seine Frage, welche Möglichkeiten es für sie böte, Europäer:innen in und außerhalb Europas zu tracken.

Was dagegen tun ?

1) Turn of AD ID in phone settings

2) Check which apps have access to location (newer phones have better controls)

3) Use a browser that is more privacy friendly and disables third party tracking

If you do these three steps you have done most important stuff.

https://twitter.com/martingund/status/1334827342011785221?s=20

Links zum Weiterlesen:

- https://nrkbeta.no/2020/12/03/my-phone-was-spying-on-me-so-i-tracked-down-the-surveillants/
- https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps
- https://www.derstandard.at/story/2000122243733/wie-standortdaten-von-einer-vermeintlich-harmlosen-wetter-app-bei-us
- https://netzpolitik.org/2020/smartphone-tracking-wie-daten-von-kommerziellen-apps-an-den-staat-gelangen/