What Surveillance Capitalism Means to You!

Information is Your Only Protection

By Rex M. Lee- Cybersecurity and Privacy Advisor/Technology Journalist,

www.MySmartPrivacy.com Rlee@MySmartPrivacy.com

My Smart Privacy™

Privacy & Data Security

Rex M. Lee

Cybersecurity & Privacy Advisor/Technology Journalist

"Success from Experience"

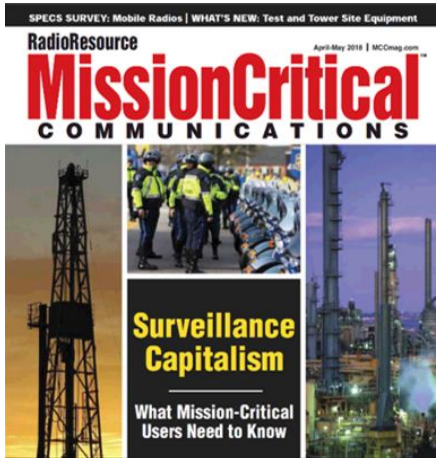
- 35 Years of Wireless Industry Experience including Platform and Application Development Experience
- Senior Executive, VP, RVP, GM & Consulting Experience
- Founder of RML Business Consulting, LLC and My Smart Privacy™
- Application Developer
- Advisor- Department of Homeland Security, National Security Agency, and The House & Senate Judiciary Committees
- Public Speaker- a) ENTELEC b) IWCE c) OilComm d) Techno Security & Digital Forensics
- Technology Journalist- The Epoch Times, MissionCritical Communications Magazine, The Wireless Messaging News and Money Masters. Published Articles- 2016, 2017, 2018, & 2019

My Smart Privacy™
Privacy & Data Security

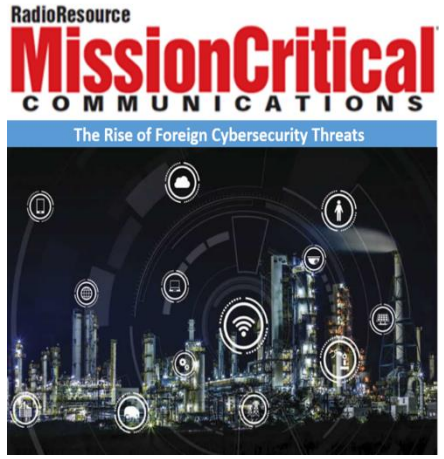
MissionCritical Communications Magazine Articles by Rex M. Lee

- Is Your Smartphone Secure?- 2017

- What Surveillance Capitalism Means For You- 2018



- The Rise Of Foreign Cybersecurity Threats- 2019



My Smart Privacy™
Privacy & Data Security

“Ever Get The Feeling That You Are Being Spied On?”

Do You Want to Get Unplugged From The Silicon Valley Matrix?

"Red Pill- Warning! If You Choose to Stay, You Will be Unplugged From The Silicon Valley Matrix"

"Blue Pill- Warning! If You Like Your Smartphone, Tablet PC & Connected Products, Please Leave Now"

Is Personal and Professional Privacy Important to You?

Would You allow 15 or More Multinational Companies, including Companies from China & Russia plus Business Competitors to Monitor, Track and Data Mine your Home & Office Phone Activity including Content 24x7/365?

Home Phone

Office Phone

My Smart Privacy™
Privacy & Data Security

Is Personal and Professional Privacy Important to You?

Would You Allow 15 or More Multinational Companies, including Companies from China & Russia plus Business Competitors to Monitor, Track and Data Mine your Home & Office PC Activity including Content 24x7/365?

Home PC

Office PC

My Smart Privacy™
Privacy & Data Security

Is Personal and Professional Privacy Important You?

Would You Allow 15 or More Multinational Companies, including Companies from China & Russia plus Business Competitors to Conduct Surveillance (Physical, Audio & Video) on your Personal and Business Activities 24x7/365?

Personal Activities

Business Activities

My Smart Privacy™
Privacy & Data Security

When You Use a Smartphone for Personal and Professional Purposes, You are in Fact Enabling 15 or More Multinational Companies, Including Companies from China & Russia plus Potential Business Competitors to Monitor, Track and Data Mine Your Personal & Professional Activities Associated with the Use of the Device 24x7/365 Days Per Year.

My Smart Privacy™
Privacy & Data Security

What is a Smartphone?

My Smart Privacy™
Privacy & Data Security

A Smart Phone is An Integrated Cellular Phone & PC That is *Supported by Protected (4th Amendment/Due Process) Telecom Infrastructure Governed by The FCC.*

My Smart Privacy™
Privacy & Data Security

Smartphones are not Private or Secure according to T-Mobile & Verizon!

My Smart Privacy™
Privacy & Data Security

Connected Products or Corporate Surveillance Tools?

"According to T-Mobile and Verizon Smartphones, Tablet PCs, Connected Products, IoT/IIoT Devices, and PCs Supported by the android OS, Apple iOS, and Microsoft Windows OS are Not Private or Secure"

T-Mobile & Verizon Admissions

Connected Products Supported By The Android OS And Apple iOS Are Not Private, Secure Or Safe Forms Of Telecommunications And Computing!

T-Mobile Admission:

"We, too, remember a time before smartphones when it was reasonable to conclude that when you activated service with T-Mobile that only T-Mobile would have access to our personal information. However, with the Samsung Galaxy Note, the iPhone, and many other devices, there are indeed a variety of parties that may collect and use information." — T-Mobile Privacy Team (FCC Consumer Complaint #423849 Filed by Rex M. Lee/Public Record- Nov 6th- 2015).

Verizon Admission:

"We have reviewed your request at the highest levels of our organization and have confirmed that the only solutions to make a phone private and secure are available through third parties, not directly from Verizon…. Additionally, Verizon is not equipped to address preinstalled solutions or applications on any device" - Verizon July 2nd, 2018

"Connected products are intentionally designed to enable the content developers with the ability to monitor, track, and data mine the product user for financial gain at the expense of the product user's civil liberties, privacy, cyber security and safety"- Rex M. Lee

Addictive and Harmful Technology

According to Google & Facebook former Executives & Product Designers, Apps & Platforms Are Intentionally Developed to be Addictive at the Expense of Privacy & Safety

Is Addictive and Harmful Technology Legal? If Not, Who is Protecting Technology Users?

My Smart Privacy™
Privacy & Data Security

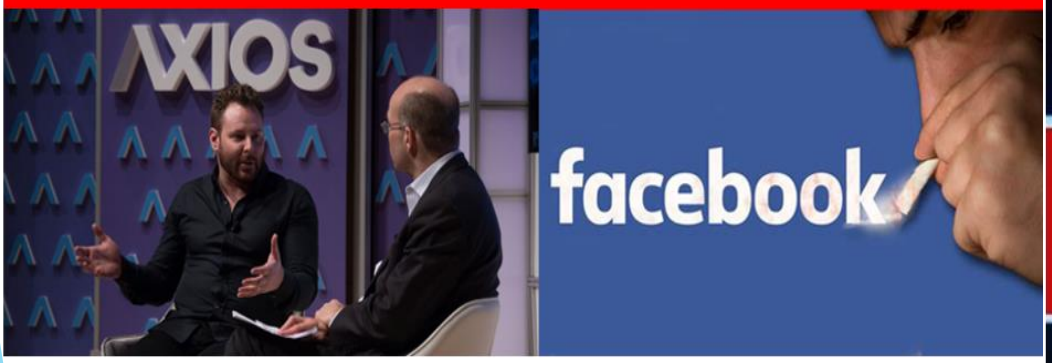
www.MySmartPrivacy.com

Addictive and Harmful Technology

According to Google & Facebook former Executives & Product Designers, Apps & Platforms Are Intentionally Developed to be Addictive evan at the Expense of Privacy & Safety!

"God Only Knows What it's Doing To Our Children's Brains..."- Sean Parker, Facebook Founder

Facebook Co-Founder, Sean Parker Admits that Facebook is Addictive and Harmful!- AXIOS Interview



Sean Parker (Co-Founder Facebook & Spotify): a) "It's a social-validation feedback loop ... exactly the kind of thing that a hacker like myself would come up with, *because you're exploiting a vulnerability in human psychology*.....*God only knows what it's doing to our children's brains*..... The inventors, creators — it's **me**, it's **Mark [Zuckerberg]**, it's **Kevin Systrom** on Instagram, it's **all of these people** — *understood this consciously. And we did it anyway*...."- Sean Parker, Axios- November 9th, 2017.

"The Average Person Checks their Smartphone 150 Times Per Day. Why Do We Do This?"- Tristan Harris, Google

Former Google Product Designer, Tristan Harris Admits Google Develops Addictive Technology- 60 Minutes/TedTalk

Tristan Harris Quotes (Former Lead Google Product Designer) A Time Well Spent: "The average person checks their phone 150 times a day. Why do we do this? Are we making 150 conscious choices? One major reason why is the #1 psychological ingredient in slot machines: intermittent variable rewards . . . Addictiveness is maximized when the rate of reward is most variable.....By shaping the menus we pick from, technology hijacks the way we perceive our choices and replaces them with new ones. But the closer we pay attention to the options we're given, the more we'll notice when they don't actually align with our true needs." Tristan Harris- 60 Minutes & TED Talk 2017

My Smart Privacy™
Privacy & Data Security

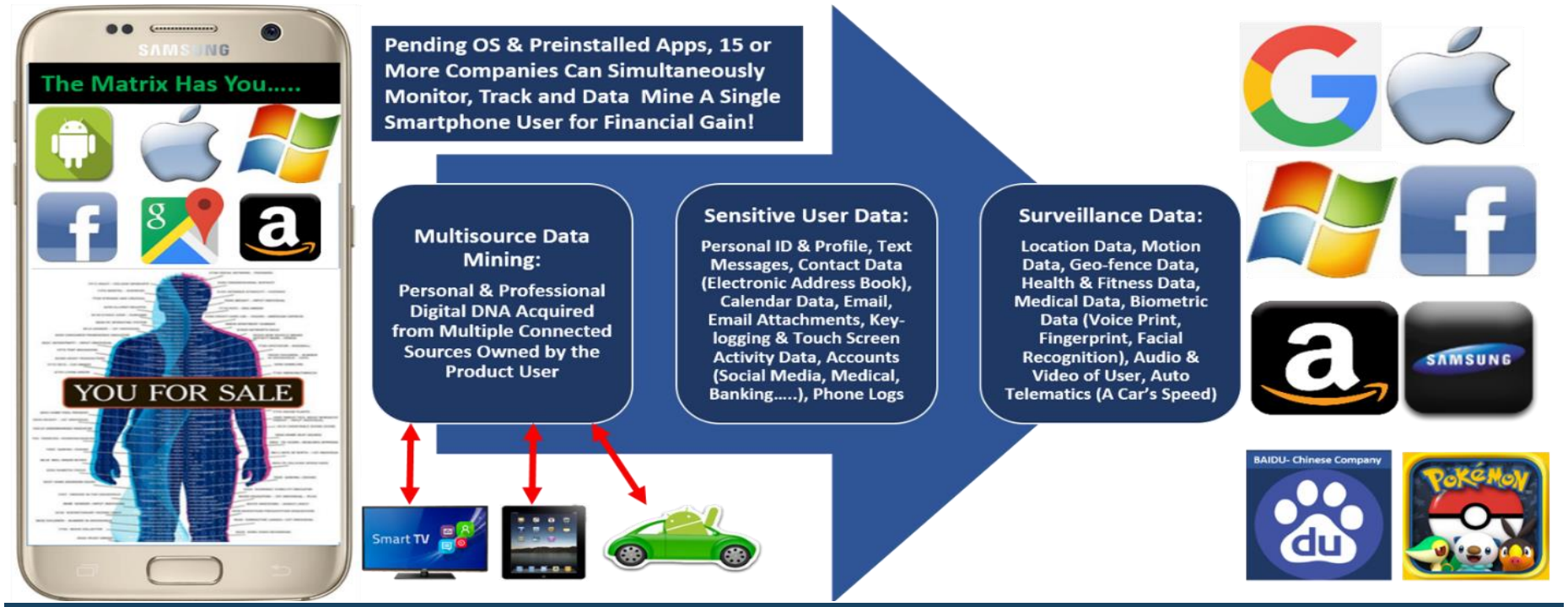
App Driven Tech and Telecom Products are Designed for Consumerism!

Tech & Telecom Products: Smartphones, Tablets, PCs, & IoT/IIoT

Connected Products: TVs, Appliances, Vehicles, & Wearables

My Smart Privacy™
Privacy & Data Security

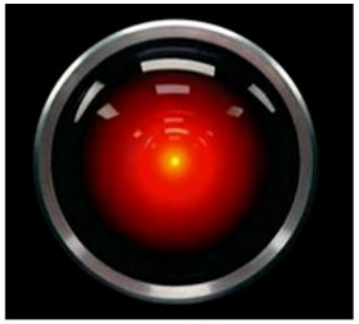
Surveillance Capitalism!

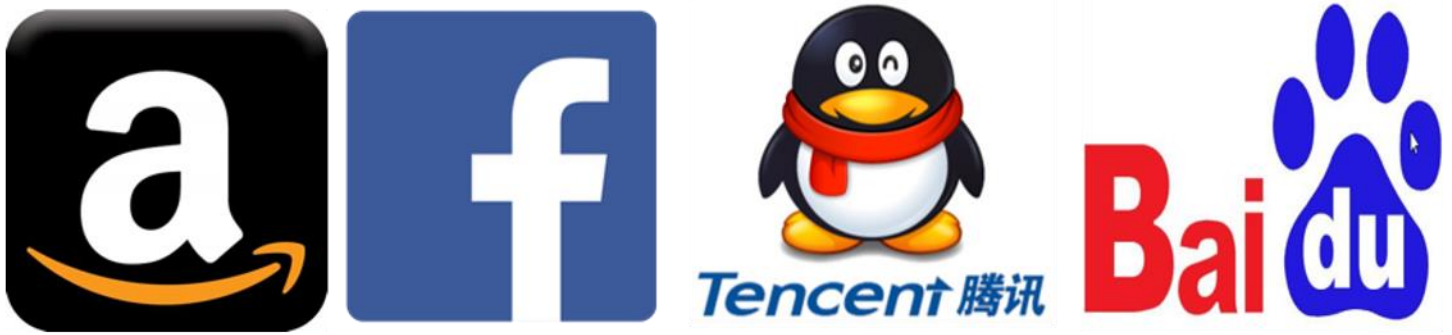


App Driven Tech and Telecom Products are Supported by Predatory Surveillance and Data Mining Business Practices Rooted in Surveillance Capitalism!

My Smart Privacy™
Privacy & Data Security

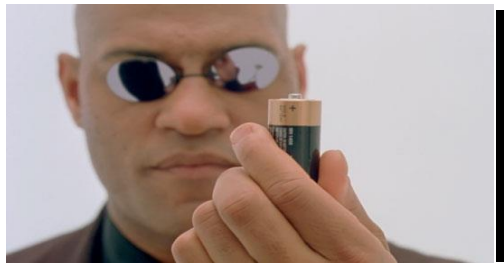
“What is Surveillance Capitalism?”





”Monetizing the Operating System User by Way of Predatory Surveillance & Data Mining Apps”

Personal & Professional Digital DNA- The New Oil



Personal & Professional Digital DNA is the Most Valuable Resource on the Planet. Tech Giants have Turned Tech & Telecom Product Users into *"Uncompensated Information Producers"* to be Exploited for Financial Gain!

Pending OS & Preinstalled Apps, 15 or More Companies Can Simultaneously Monitor, Track and Data Mine A Single Smartphone User for Financial Gain!

Multisource Data Mining:

Personal & Professional Digital DNA Acquired from Multiple Connected Sources Owned by the Product User

Sensitive User Data:

Personal ID & Profile, Text Messages, Contact Data (Electronic Address Book), Calendar Data, Email, Email Attachments, Key-logging & Touch Screen Activity Data, Accounts (Social Media, Medical, Banking.....), Phone Logs

Surveillance Data:

Location Data, Motion Data, Geo-fence Data, Health & Fitness Data, Medical Data, Biometric Data (Voice Print, Fingerprint, Facial Recognition), Audio & Video of User, Auto Telematics (A Car's Speed)

My Smart Privacy™
Privacy & Data Security

Tech and Telecom Product User Exploitation

When You Use Your App Driven Tech and Telecom Products, You Produce the New Oil in the Form of Personal and Professional Digital DNA which is Collected by the App Developer to Exploit for Financial Gain at the Expense of the App User's Civil Liberties, Privacy, Cybersecurity & Safety!

Intrusive Apps Support Tech, Telecom, & Connected Products

Tech & Telecom Products: Smartphones, Tablets, PCs, & IoT/IIoT

Connected Products: TVs, Appliances, Vehicles, & Wearables

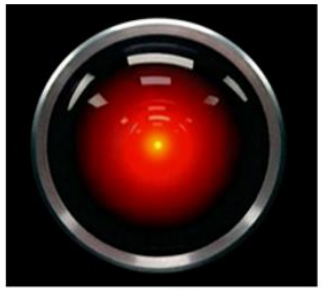
My Smart Privacy™
Privacy & Data Security

When You See Apps, You See Necessity, Convenience, & Entertainment!

My Smart Privacy™
Privacy & Data Security

www.MySmartPrivacy.com

When I See Apps, I See Legal Malware Supported by Exploitive Terms of Use!



Apps are Intentionally Designed to Enable the App Developer with the Ability to Monitor, Track and Data Mine the App and/or Platform User for Financial Gain!

My Smart Privacy™
Privacy & Data Security

Legal Malware in the Form of Apps Supported by Exploitive T&Cs

Methods Used by Content Developers to Harvest a Person's Digital DNA

Published (Online) Terms of Use-

- Terms and Conditions ("T&Cs")
- Privacy Policies
- End User Licensing Agreements ("EULAs")

Preinstalled ("Rooted") Unpublished (Hidden in Device) Terms of Use*-

- Application Permission Statements
- Application Product Warnings
- Interactive Application Permission Command Strings

**Unpublished Terms of Use may violate existing consumer laws governed by State AGs and the FTC due to hidden legalese, product warnings, misleading legalese and combined pages of text*

Collective Terms of Use & Preinstalled Content-

- Pending the OS, preinstalled content and number of preinstalled content developers, the collective terms of use can exceed **3,000 pages** of complicated legalese
- Terms of Use do Not indemnify (protect) the product user from harm
- Pending OS, as many as 300 or more apps, widgets, emojis and other content is preinstalled into connected products such as smartphones
- Pending OS, as many as **15 or more companies** can be responsible for the development of the preinstalled content that supports connected products
    - Pending OS, as many as **15 or more multinational entities** from around the world are enabled to ***simultaneously*** monitor, track & data mine the product user for financial gain
- The collective legalese is intentionally written to be "Torturous" so that the product user simply clicks on "I Agree" without reading the fine print
- The legalese is intentionally written in a manner that enables numerous multinational entities with ability to monitor, track and data mine the product user for financial gain

My Smart Privacy™
Privacy & Data Security

Predatory Terms of Use & Intrusive Preinstalled & Third-party Content!

Methods Used by Content Developers to Harvest a Person's Digital DNA

Personal Identification- Users are Identified by Content Developers!

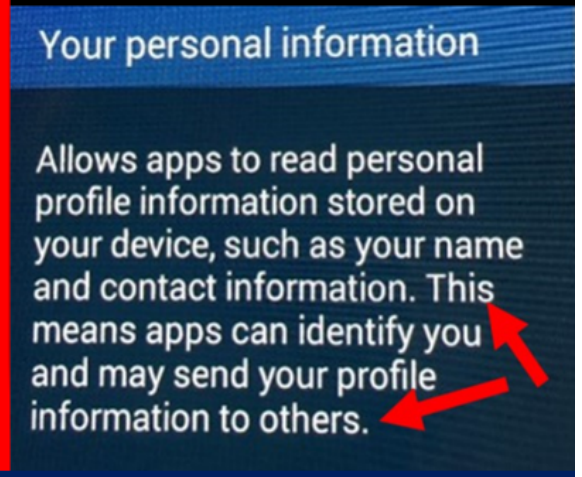
Misleading and Contradictive Legalese Associated with Published & Unpolished Terms of Use

Google Published (Online) Privacy Policy- 2018

Google Privacy & Terms

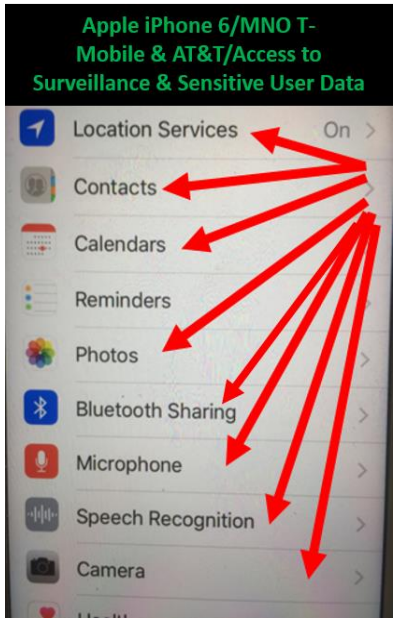
We may share non-personally identifiable information publicly and with our partners — like publishers, advertisers, developers, or rights holders. For example, we share information publicly to show trends about the general use of our services. We also allow specific partners to collect information from your browser or device for advertising and measurement purposes using their own cookies or similar technologies.

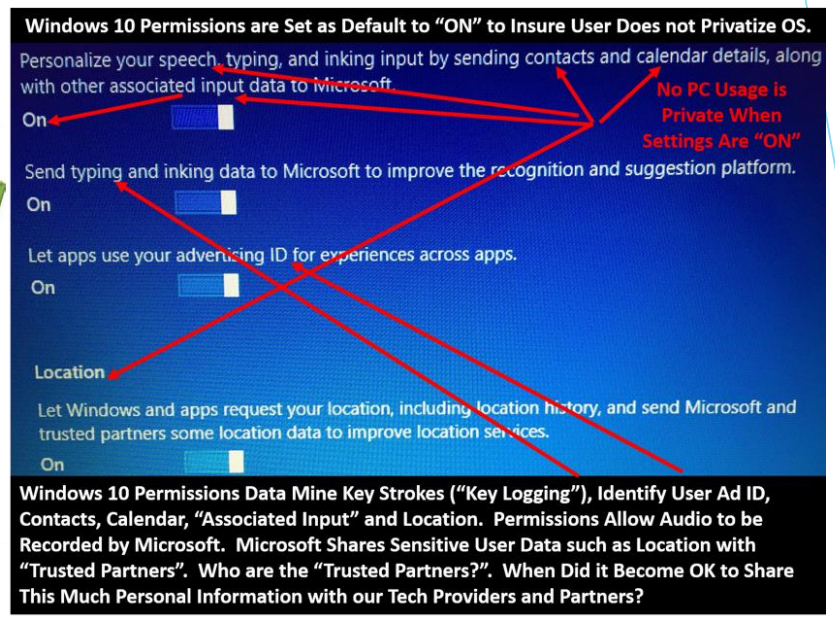
Samsung Galaxy Note 2- android Jelly Bean OS/MNO T-Mobile/Personal ID

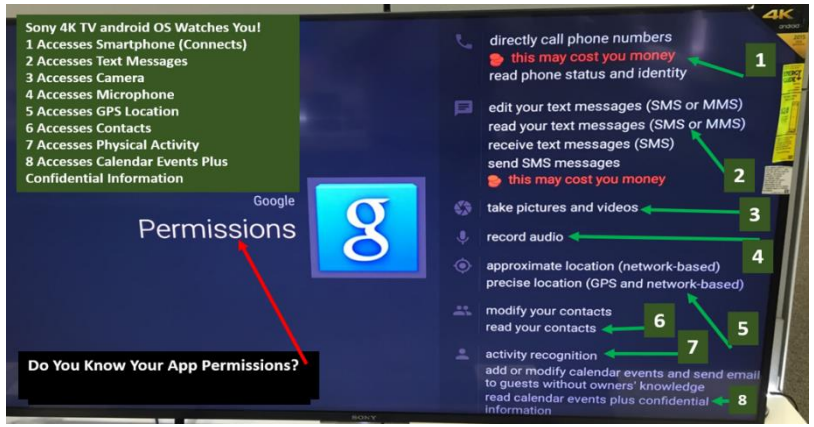


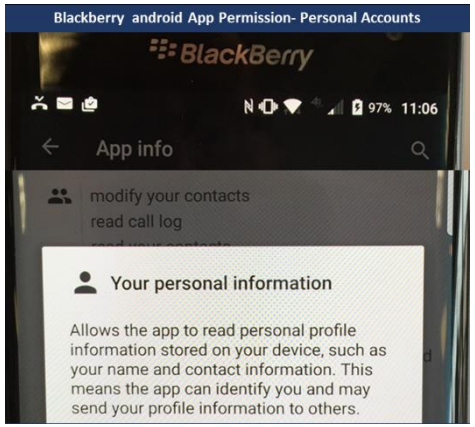
The Google privacy policy implies that the device user's personal identity is protected ("Non-personally"). However, the unpublished (hidden in device) preinstalled android legalese (Personal Profile App Permission) clearly states that the preinstalled apps do in fact identify the telecom subscriber ("paying customer") or authorized device user (spouse, child, etc.). The android app permission also enables the third-parties to share the user's ID and profile with "others".

Apple, Microsoft, Sony & Blackberry Examples!
No Product is Private, Secure or Safe- Smartphones, Tablets, TVs, Autos, PCs and so On……





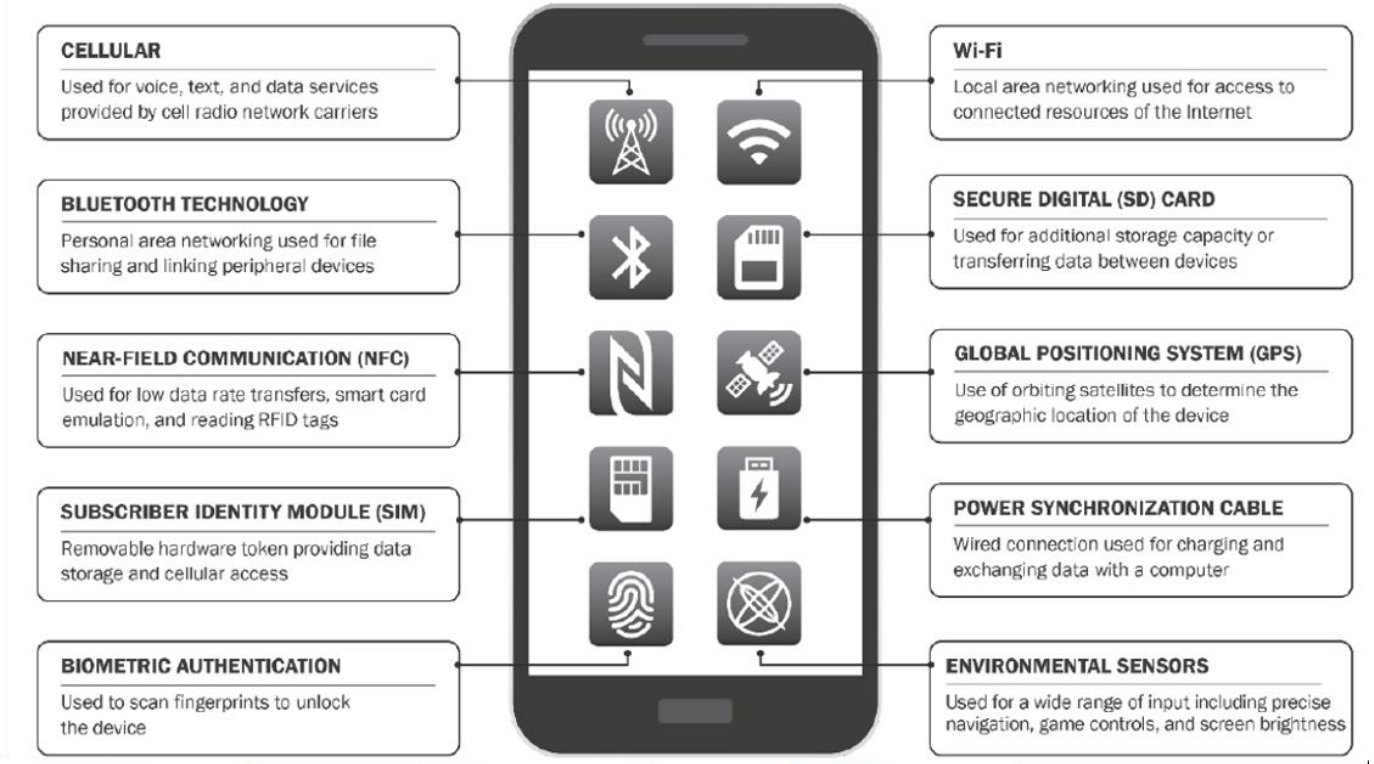




My Smart Privacy™
Privacy & Data Security

Device Control

OS & App Developers are Enabled to Take Full Control Over the Smartphone, Tablet PC, Connected Product or PC!



My Smart Privacy™
Privacy & Data Security

Digital DNA Acquisition Flow Chart
Personal & Professional Information Collected by Apps

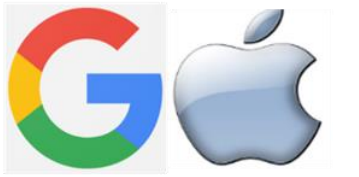
Digital DNA Acquisition Flow Chart- Connected Products Supported by the android OS, Apple iOS & Microsoft Windows OS

Pending OS & Preinstalled Apps, 15 or More Companies Can Simultaneously Monitor, Track and Data Mine A Single Smartphone User for Financial Gain!

Multisource Data Mining:
Personal & Professional Digital DNA Acquired from Multiple Connected Sources Owned by the Product User

Sensitive User Data:
Personal ID & Profile, Text Messages, Contact Data (Electronic Address Book), Calendar Data, Email, Email Attachments, Key-logging & Touch Screen Activity Data, Accounts (Social Media, Medical, Banking.....), Phone Logs

Surveillance Data:
Location Data, Motion Data, Geo-fence Data, Health & Fitness Data, Medical Data, Biometric Data (Voice Print, Fingerprint, Facial Recognition), Audio & Video of User, Auto Telematics (A Car's Speed)



A Person's Personal and Professional (Employment) Digital DNA is Comprised of Surveillance Data (E.G. Location Data), Sensitive User Data and Digital DNA Acquired from Multiple Connected Sources Owned by the Product User.

My Smart Privacy™
Privacy & Data Security

Digital DNA Acquisition Summary Detail
Personal and Professional Information- Surveillance & Sensitive User Data

Digital DNA Acquisition Summary (Application Legalese/Permissions)- Personal and Professional Information/Android OS (Google), Apple iOS, & Microsoft Windows OS								
Sensitive User Data:	Personal ID- App Developers Identify Users	Messaging- SMS Text, Instant, Social Media, Etc.	Email- Content & Attachments	Contacts (Electronic Address Book)- Personal & Professional Contacts	Calendar Data- Events, Tasks, Alarms, Coworkers, Notes	Logs- Phone, Messaging, App Usage History, Notifications Etc.	Caller ID- Incoming/Outgoing Calls Including Device ID	Web & Bookmark History- Browsing, Etc.
Accounts- Access to Accounts Setup on Device Without Consent or Knowledge:	Medical- Patient Portals, Pharmacy, Etc.		Banking- Personal & Professional	Social Media- LinkedIn, Facebook, Twitter, Instagram, Etc.	Internet- Amazon, Walmart, Macey's, Etc.	Business- Includes All Accounts Set up on Device	Personal- Includes All Accounts Setup on Device	
Files- Access to Files & Media Without Consent or Knowledge:	Files in General	Entertainment- Music, TV, Movies, News, Programming in General		Photos Shot by User	Video Shot by User	Audio Recorded by User	Visual Voicemail- Voice Mail Accessed by Visual Voicemail App	
Multi-Source Data Mining- Sources Connected to Host Device Without Consent or Knowledge:	USB- External Hard Drives, Thumb Drives	PCs- Tablets, Desktop, Lap Top, Etc.	Connected Products- TVs, Appliances, Climate Control, Security Systems	Automated Voice Assistants- Amazon Alexa, Apple Siri, MS Crotona, Google Assistant	Connected Vehicles- Autos, Trucks, Etc.	IoT/IIoT Devices	RF Devices- 4/5G Smartphones, Feature Phones ("Flip"), LMR, Wi-Fi, Etc.	Unrelated Digital DNA- Collection of Sensitive User, Surveillance, Biometric and Other Data Not Associated with the Use of App, Product or Platform
Multisource Surveillance Data- Location Data:	GPS- Precise Data Coordinates	Cell Towers- Track 4/5G Users by Cell Sites Including Micro-Cell Sites	Wi-Fi Access Points ("APs")	Nearfield Communication ("NFC")- Tags, Beacons, Google & Apple Pay, Etc.	Geo-Fence Data- Time Stamp of Arrival & Departure Tied to Exact Location Data	Motion Data- Stationary, Walking, Running, Cycling, Vehicle	Contact Tracking- Emails, Phone, Messaging, & Other Forms of Contact	Bluetooth
Biometric Data:	Facial	Voice Print/Recognition	Medical, Health & Fitness Data- Heart Rate, Blood Pressure, Blood (Diabetes), Etc.	Fingerprint	Eye- Retina Data	Blood/DNA Data		
Video & Audio Surveillance- Surveillance Without User Consent or Knowledge:	Camera	Microphone						
Device Control- Control Without User Consent of Knowledge:	Lock screen & Password- Disable All Passwords	Biometric Authentication	Multisource Tracking: GPS, Cell Towers, Wi-Fi AP & NFC	Power-Keep Device from Sleeping	Hardware- Camera, Microphone, Volume Control, Etc.	Preinstalled & Third-Party Content Control- Run Apps at Start-up, Reboot or OS Up-date	Default to Original Settings at Reboot, OS Up-dates, Power, Etc.- Content (Apps, Widgets, Etc.)	Network Connectivity Control- Auto Connect to the Internet by 4/5G/Wi-Fi/NFC, Bluetooth, Etc. Without Consent	Auto Import/Export Control- Files, Data, Messaging, Etc..

My Smart Privacy™
Privacy & Data Security

The Top Ten Internet Companies in The World- U.S. & China

Amazon	$232 Billion	USA
Google	$120 Billion	USA
JD.Com	$67 Billion	China
Alibaba	$56 Billion	China
Facebook	$55 Billion	USA
Tencent	$44 Billion	China
Netflix	$15 Billion	USA
Bookings	$12 Billion	USA
Baidu	$12 Billion	China
e-Bay	$10 Billion	USA

*Source Wikipedia

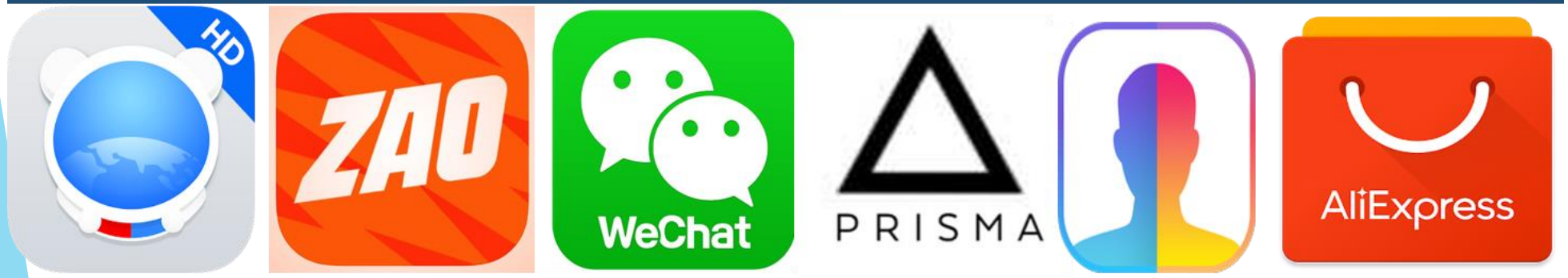
You Are For Sale By: Google, Apple & Microsoft!

The Conduit to the Tech & Telecom Product User is the Operating System

Google, Apple, and Microsoft Does Note Sell Your "Identifiable" Personal and Professional Information, they Sell Access to You by way of Intrusive Apps Developed by Third-Party & Preinstalled App & Platform Developers, Including Developers from China & Russia:

Google, Apple, & Microsoft Distribute Chinese & Russian Surveillance & Data Mining Technology via Google Play, Apple App Store & Microsoft App Store

Chinese & Russian Malware: Surveillance & Data Mining Apps



App Developers Access: Biometric Data, Contacts, Photos, Text Messages, Location Data, Voice & Video Recordings, Calendar Data, Instant Messages, Photos, Files, and So On.....

WeChat App Analysis- Tencent China
Distributed Through Google Play, The Apple App Store, & Microsoft App Store

App permissions

Applies to: Windows 10

WeChat For Windows

Tencent WeChat Limited • Social

Some apps or games in Microsoft Store are designed to take advantage of specific hardware or software capabilities on your Windows device. A photo app might need to use your phone's camera, or a restaurant guide might use your location to recommend nearby places.

In Windows 10, use the Privacy page to choose which apps can use a particular feature. Select **Start** > **Settings** > **Privacy**. Select the app (for example, Calendar) and choose which app permissions are on or off.

The Privacy page won't list apps with permission to use all system resources. You can't use the Privacy settings to control what capabilities these apps can use. Windows Desktop apps fall under this category. To see the permissions for an app, go to the app product page in Microsoft Store or online. If you don't want an app to use any of the features listed, you can choose not to install it.

Here's more info on what permissions allow an app to do:

All system resources: Use any and all system resources (such as camera, microphone, or location) without further notification. You can't control app permissions for individual system resources via the Privacy page.

Account Info: Access any of your account info.

Bluetooth: Activate and use any Bluetooth connections between your device and other devices.

Contacts: Access your contacts, people, or address book apps.

Calendar: Access your calendars.

Call History: Access history of phone calls you made on the device, in Skype or other telephony apps.

Email: Access your email and account info for your email accounts.

Facial recognition: Activate and use any facial recognition hardware.

Fingerprint reader: Activate and use any fingerprint reader hardware.

Location: Activate and use the GPS or other location-finding features on your device. Access location data in Maps and other location apps.

Google Play | WeChat - Free messaging and | App permissions - Windows He | Get BaiduBrowser - Microsoft S

...port.microsoft.com/en-us/help/10557/windows-10-app-permissions

Location: Activate and use the GPS or other location-finding features on your device. Access location data in Maps and other location apps.

Messaging: Access your instant messages and account info.

Microphone: Activate and use the microphone on your device.

Motion: Activate and use the accelerometer or other motion-sensing feature on your device.

Music library: Access any music files from the Music library on your device.

Near field communications: Activate and use any near field communications (NFC) connections between your device and other devices.

Notifications: Access your notifications, found in action center.

Pictures library: Access any picture files from the Pictures library on your device.

Tasks: Access your task list in Outlook and other task-tracking apps.

Video library: Access any video files from the Video library on your device.

Voice recognition: Activate and use any voice recognition hardware.

Webcam: Activate and use the camera on your device.

WiFi: Activate and use WiFi connections between your device, the internet, and other devices.

Wired connections: Activate and use any wired connections, including Ethernet, USB, and Serial communications between your device, the internet, and other devices.

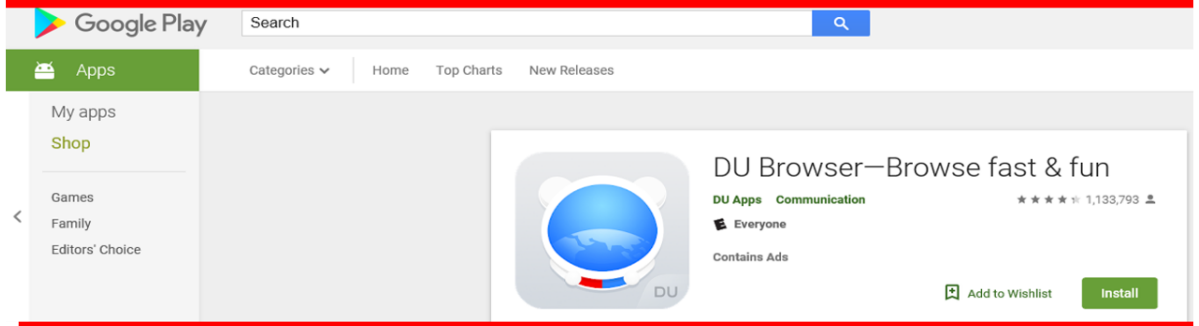
Google, Apple & Microsoft Enable Nation-state Chinese Company Tencent to Surveil and Data Mine android, Apple, & Windows 10 OS Product Users by Way of Popular Messenger App WeChat

My Smart Privacy™
Privacy & Data Security

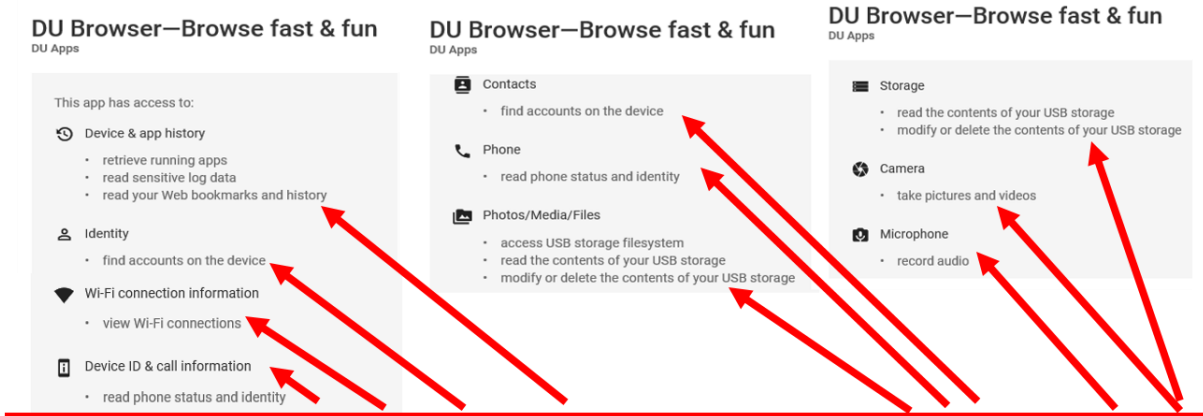
www.MySmartPrivacy.com

DU Browser App Analysis- Baidu China Distributed Through Google Play

Google Distributes Chinese Surveillance and Data Mining Technology in The Form of an App Centered on Fast and Fun- BAIDU



Google Enables BAIDU to Monitor, Track and Data Mine U.S. Citizens Including Children, Business Professionals, Govt. Officials, Govt. Employees and Even Law Makers

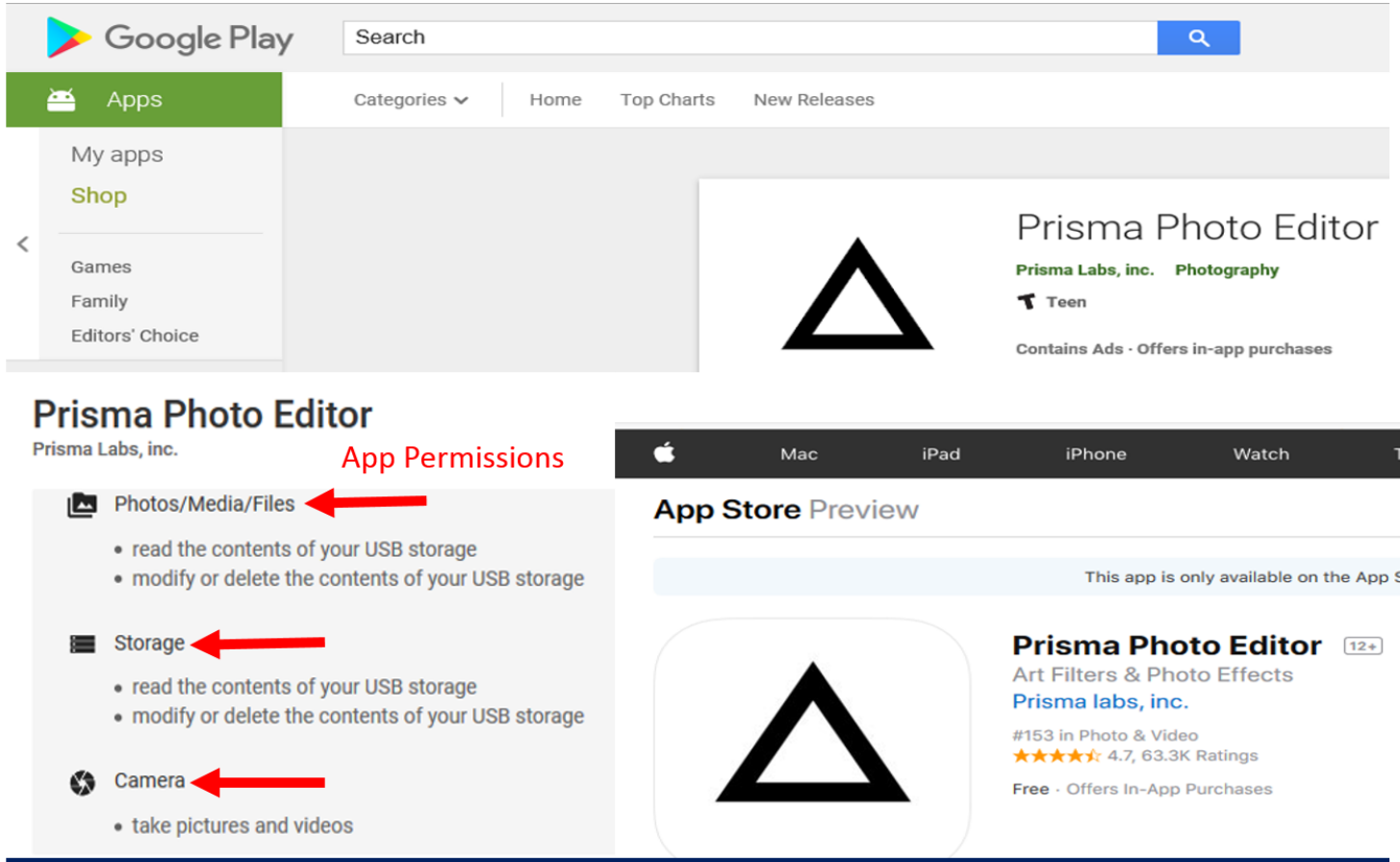


Google Enables BAIDU to Record Audio, Video and Take Pictures of the Product User Without Consent. Google Enables BAIDU to Collect User Account Info, Contacts, Phone Logs, Phone ID, Files, Photos, Music, Videos and other Highly Confidential Sensitive User Data. Google Enables BAIDU to Conduct Multisource Location Tracking via Access to Networks such as Wi-Fi via Full Network Aceess.

My Smart Privacy™
Privacy & Data Security

Prisma Photo Editor App Analysis- Prisma Labs Moscow Russia
Distributed Through Google Play and The Apple App Store- Russia

Google & Apple Enable Prisma Labs (Moscow) to Collect Photos, Media, Files plus other Info while Data Mining any Device including PCs that are Connected to the Smartphone.

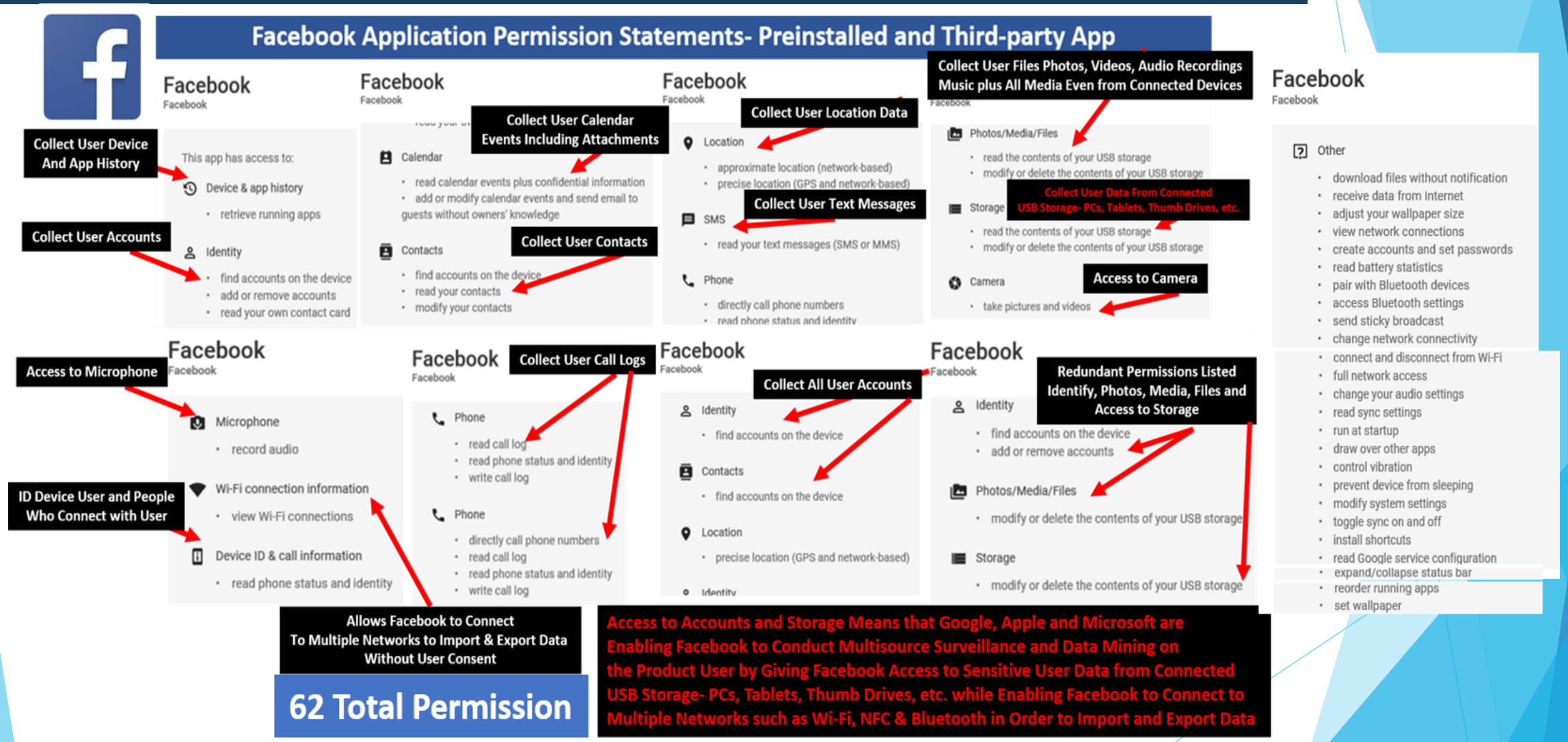


Google & Apple Enable Prisma Labs to Control Hardware such as the Camera to Take Pictures plus Record Audio & Video without the User's Knowledge or Consent.

My Smart Privacy™
Privacy & Data Security

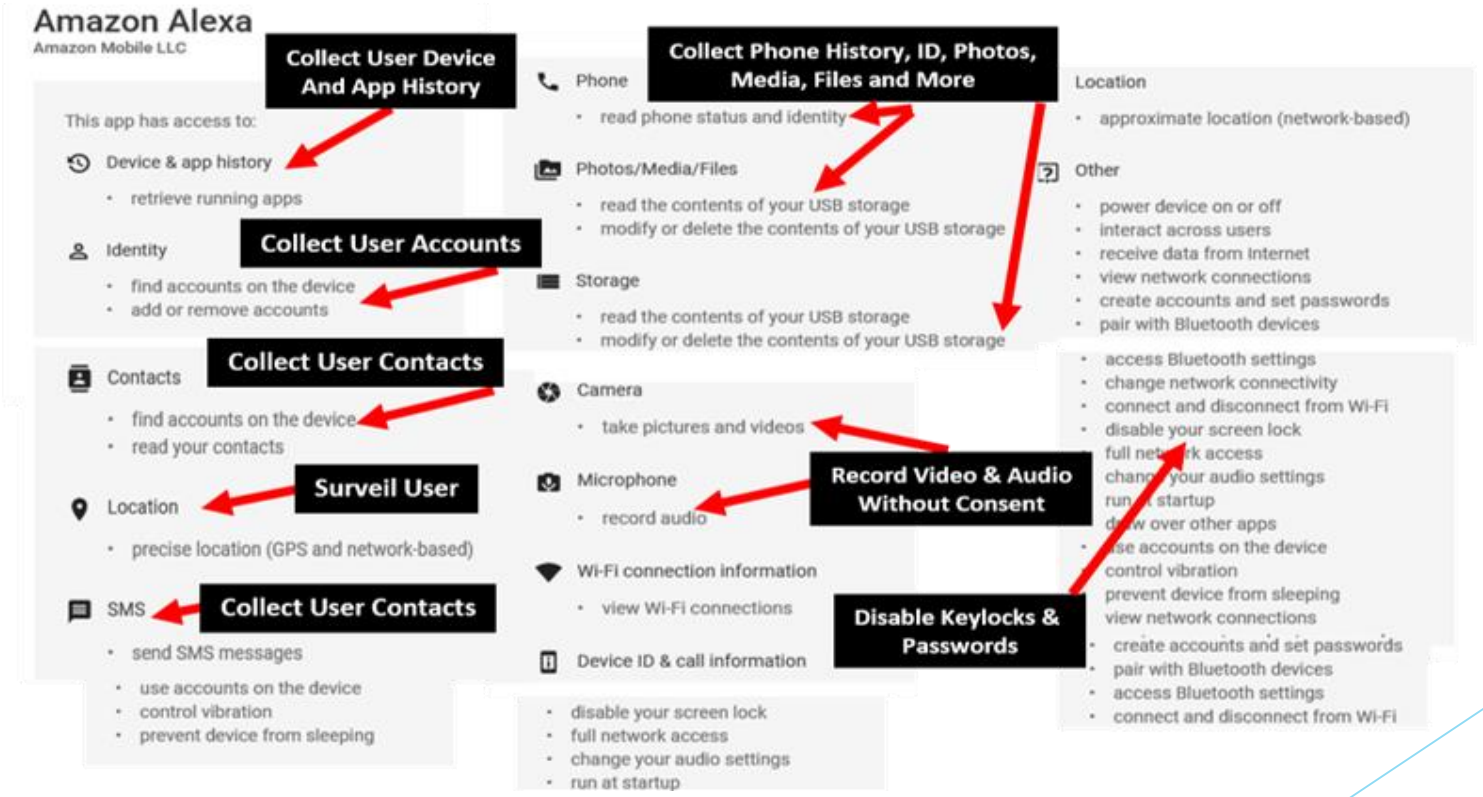
Apps Analysis- Facebook & Amazon Examples

Content Developers use Apps to Harvest Surveillance Data (e.g. Location Data) & Sensitive User Data Collectively known as a Person's Personal & Professional Digital DNA



My Smart Privacy™
Privacy & Data Security

Apps Analysis- Cont.
The Amazon Alexa App Enables Amazon to Collect More Than Your Verbal Conversations!



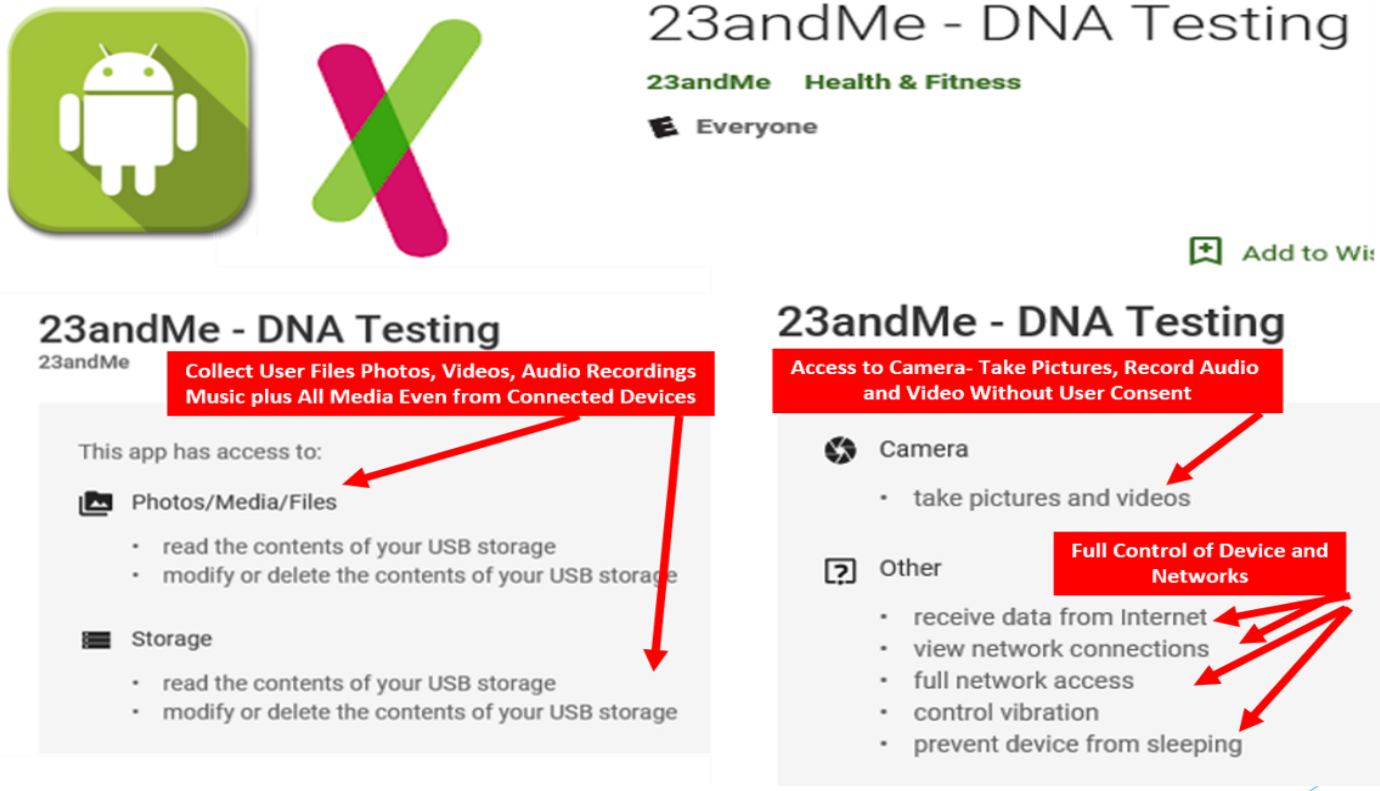
My Smart Privacy™
Privacy & Data Security

Apps Analysis- Cont.
23andMe Collects Personal & Professional Info Aside from DNA

Preinstalled & Third-party Surveillance & Data Mining Technology- Biometric Data Acquisition Apps

Physical DNA Example:

Biometric DNA- 23andMe Android App Permissions
Silicon Valley Tech Giants and DNA Companies Want Your Personal & Professional Information and Your Blood!



My Smart Privacy™
Privacy & Data Security

Android (Google) Interactive Application Permission Command String Analysis- Baidu China

Unpublished Application Legalese- Interactive Application Permission Command Strings

Uncontrollable Preinstalled Interactive Application Permission Command Strings

Chinese Surveillance Technology Example- Samsung Galaxy Note (android Jelly Bean OS)

My Smart Privacy™
Privacy & Data Security

Harmful Use of Personal & Professional Digital DNA!

Apple CEO Tim Cook poses for a selfie with journalist Britta Weddeling during a launch event in Cupertino, California, on Sept. 12, 2018. (NOAH BERGER/AFP/Getty Images)

Government Fails to Enforce Privacy, Telecommunication, and Consumer Laws Meant to Protect Citizens

Rex M. Lee

Google CEO Sundar Pichai testifies during a House Judiciary Committee hearing on Capitol Hill on Dec. 11, 2018. (Saul Loeb/AFP /Getty Images)

Facebook and Google Congressional Hearings: Meaningless Resolve and Phony Apologies

Rex M. Lee

My Smart Privacy™
Privacy & Data Security

Harmful Use of Telecom Related Personal & Professional Digital DNA

"How is Telecom Related Personal and Professional Digital DNA being Used, Share, Sold, Purchased, and Aggregated by All Parties Concerned?"

Misuse of Telecom Related Personal and Professional Digital DNA

- AI, Predictive Analytics and Suggestive Technology (E.G. Facebook Cambridge Analytica)
- Data Brokers
- Business Competitors (Foreign/Domestic)
- Employers (Current/Future)
- State Actors (Foreign/Domestic)- Nation-state Companies from Adversarial Countries
- Bank & Insurance Underwriters
- Law Enforcement (Foreign/Domestic)
- Political Use of Personal & Professional Digital DNA
- Institutions of Higher Learning
- And the List Goes On……

My Smart Privacy™
Privacy & Data Security

Is Your IP and Business Data Ending up in the Hands of Competitors?

List of Industries Plus Mergers & Acquisitions by Top Internet Companies, App, & Platform Developers:

Tech Giants Compete in Hundreds of Industries World Wide Yet are Enabled by the FTC, FCC, DOJ, DHS, and other Agencies to Monitor, Track and Data Mine People by Way of Telecom Devices & PCs Supported by Protected Telecom Infrastructure Regulated by the FCC

- Alphabet Inc. (Google) over 200 dating back to 2001
  - *Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Alphabet*
- Alibaba Industries Includes Entertainment, E-Commerce & Retail Platforms, Cloud Computing & AI, Financial Services, Internet Services, and So On……..
  - Source Wikipedia https://en.wikipedia.org/wiki/Alibaba_Group
- Apple over 100 dating back to 1988
  - *Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Apple*
- Microsoft over 200 dating back to 1987
  - *Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Microsoft*
- Facebook has been involved with over 75 mergers and acquisitions since 2005
  - *Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Facebook*
- Tencent out spent Alibaba and Baidu regarding mergers and acquisitions. Industries Include Gaming, Entertainment, Film, Social Media, Television, Comics, Publishing, Music, E-Commerce, and So On…… : https://www.scmp.com/business/companies/article/2098548/tencent-leads-baidu-alibaba-when-it-comes-ma-deals
  - Source Wikipedia: https://en.wikipedia.org/wiki/Tencent
- Amazon over 90 since 1998
  - *Source Wikipedia: https://en.wikipedia.org/wiki/List_of_mergers_and_acquisitions_by_Amazon*

- **And the List Goes On……**

My Smart Privacy™
Privacy & Data Security

Intrusive & Malicious Apps can Launch Attacks on Networks!

Hands on a keyboard in front of a displayed cyber code on Oct. 4, 2018. (Reuters/Dado Ruvic/Illustration/File Photo)

Chinese and Russian Companies Exploit Flaws in US Cybersecurity

Are Google and Apple violating US sanctions against Russia?

Rex M. Lee

Intrusive & Malicious Apps Threaten Cybersecurity Including Network Infrastructure

Google removes 300 Android apps that secretly hijacked phones for DDoS attacks

The Google Play apps offered services including storage managers, ringtones

By Thuy Ong | @ThuyOng | Aug 29, 2017, 4:29am EDT

SHARE

Photo by Amelia Holowaty Krales / The Verge

AD

MOST REA

The 2019 Oscars broke new

Weakness in Apple MDM Tool Allows Access to Sensitive Corporate Info

Author:
Lindsey O'Donnell

September 27, 2018
/ 10:49 am

3:30 minute read

Write a comment

Share this article:

Apple iOS apps subject to man-in-the-middle attacks

Apple removes malicious programs after first major attack on app store

Several apps infected by malware dubbed XcodeGhost in first case of large numbers of malicious software making their way past Apple's defences

▲ Apple products on display in its new store in the Belgian capital Brussels at the weekend. Photograph: Isopix/Rex Shutterstock

Apple has had to remove more than 300 malware-infected apps from its app store after a tainted version of its developer tools led to a number of Chinese apps leaking users' personal information to hackers.

Android Apps Susceptible to Man-in-the-Middle Attacks

BY JARED HOWE · SEPTEMBER 11, 2014

My Smart Privacy™
Privacy & Data Security

MDM & Security Apps- Verizon Admission:

MDM & Security Apps do not Protect Against Preinstalled Surveillance & Data Mining Technology Developed by Google, Apple, & Microsoft

*"**Verizon Admission** "We have reviewed your request at the highest levels of our organization and have confirmed that the only solutions to make a phone private and secure are available through third parties, **not directly from Verizon**…. Additionally, Verizon is not equipped to address **preinstalled solutions or applications on any device**" - July 02, 2018*

A man walks past a Baidu booth on Nov. 6, 2018, at the Light of Internet Expo ahead of the fifth World Internet Conference in Wuzhen in China's eastern Zhejiang province. (STR/AFP/Getty Images)

Google Distributes Surveillance Technology Developed by Chinese Company

Rex M. Lee

A monorail train plastered with a Google advertisement passes a giant sign from Apple on a building as preparations are underway for the CES 2019 show, Jan. 6, 2019, in Las Vegas, Nevada. Apple is taking a shot at rivals such as Google on the data privacy front with the message reading "What happens on your iPhone stays on your iPhone." (ROBYN BECK/AFP/Getty Images)

Apple's CES Privacy Claim Is Misleading

Apple sells Google access to its product users

Rex M. Lee

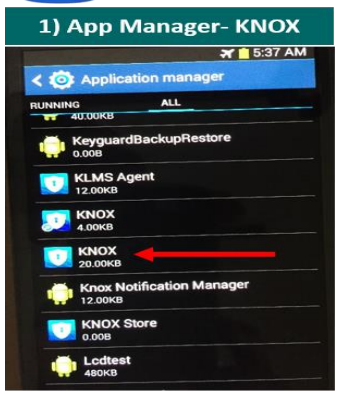
My Smart Privacy™
Privacy & Data Security

Apps Analysis
Leaky Mobile Device Management ("MDM") & Security Apps

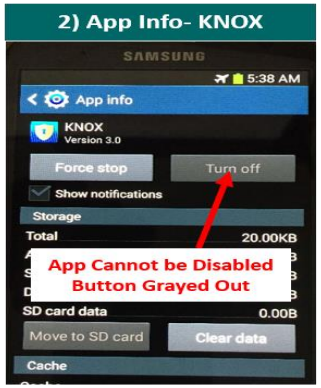
Preinstalled & Third-party Mobile Device Management ("MDM") & Security Apps Cannot Privatize or Secure a Connected Product in Regards to Preinstalled Surveillance & Data Mining Technology.

Samsung KNOX android APP- Predatory, Surveillance, Control, and Intrusive Syncing Capabilities Analysis Samsung Galaxy Note Smartphone- App Cannot be Disabled by User

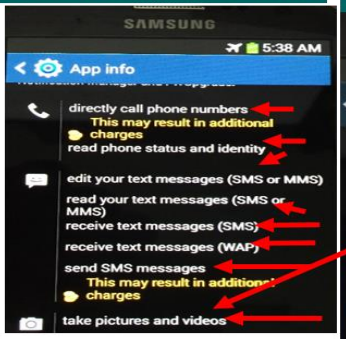
1) App Manager- KNOX



2) App Info- KNOX

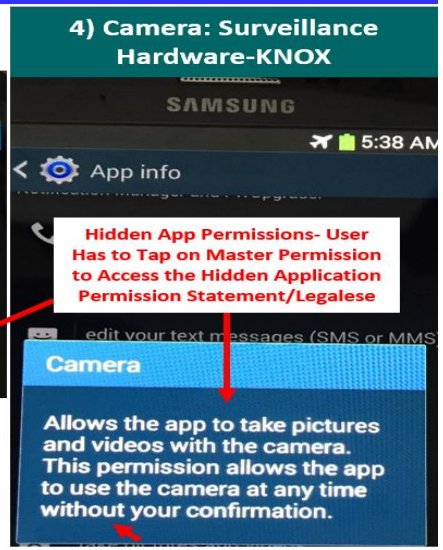


3) 68 App Permissions - KNOX

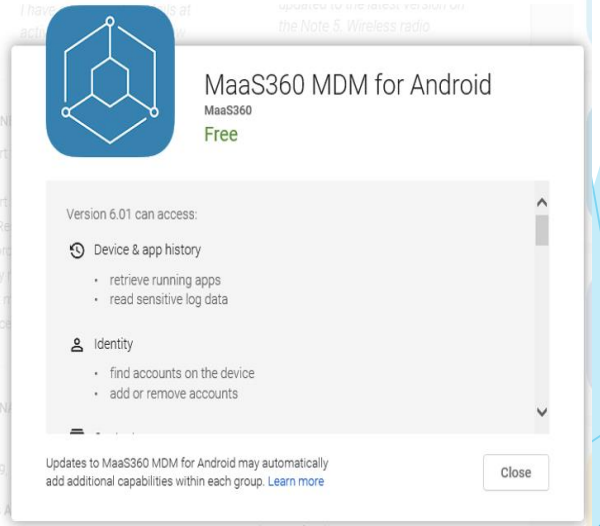


KNOX is Granted 68 Predatory, Surveillance, Control, & Intrusive Syncing android App Permissions. Google, Samsung, & Partners Can Access Nearly 100% of All Connected Product User Data via KNOX Permissions.

4) Camera: Surveillance Hardware-KNOX



IBM MaaS360

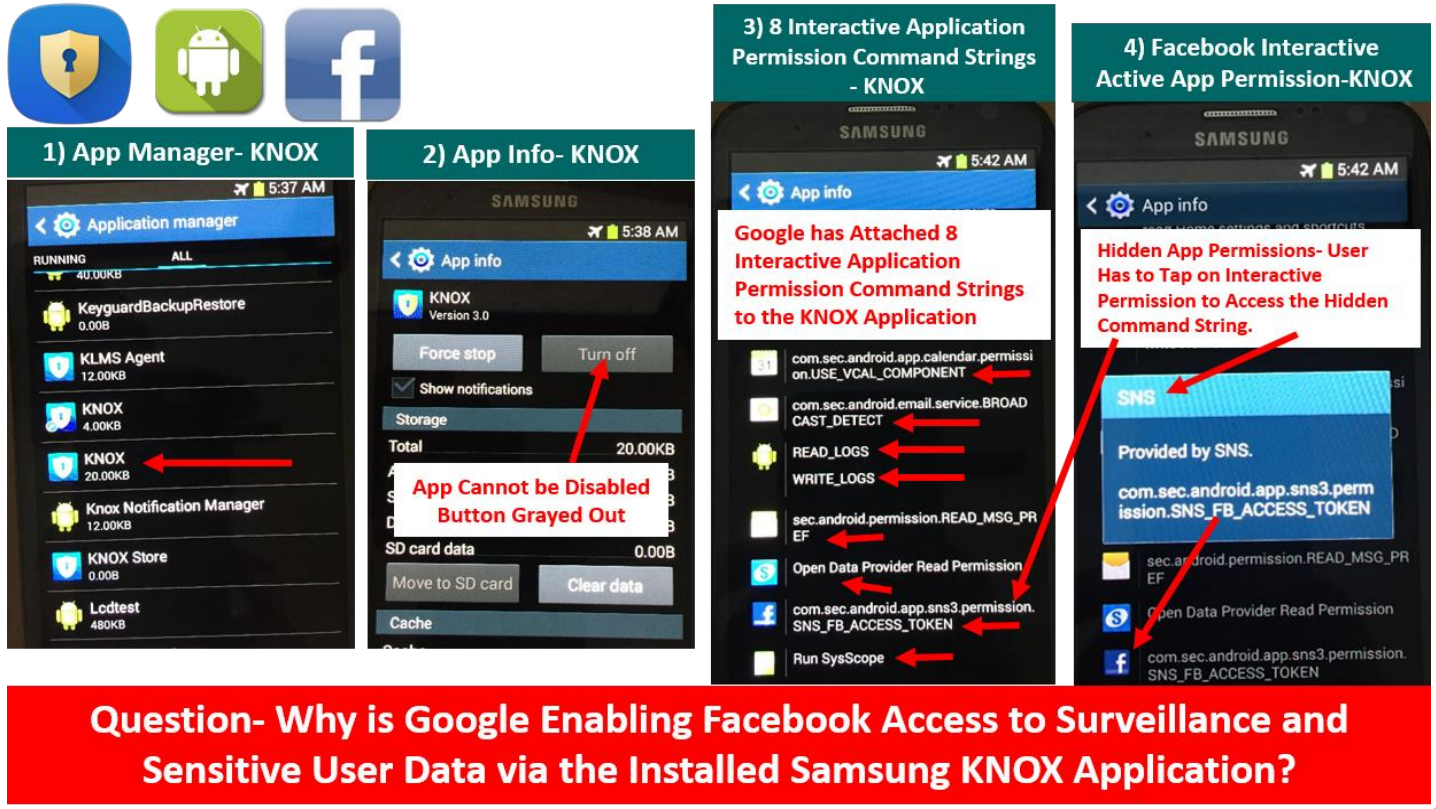


My Smart Privacy™
Privacy & Data Security

Apps Analysis- Cont.
Leaky Mobile Device Management ("MDM") & Security Apps

Preinstalled & Third-party Mobile Device Management ("MDM") & Security Apps Cannot Privatize or Secure a Connected Product in Regards to Preinstalled Surveillance & Data Mining Technology. Security apps such as KNOX Share Data with Third-parties such as Facebook:

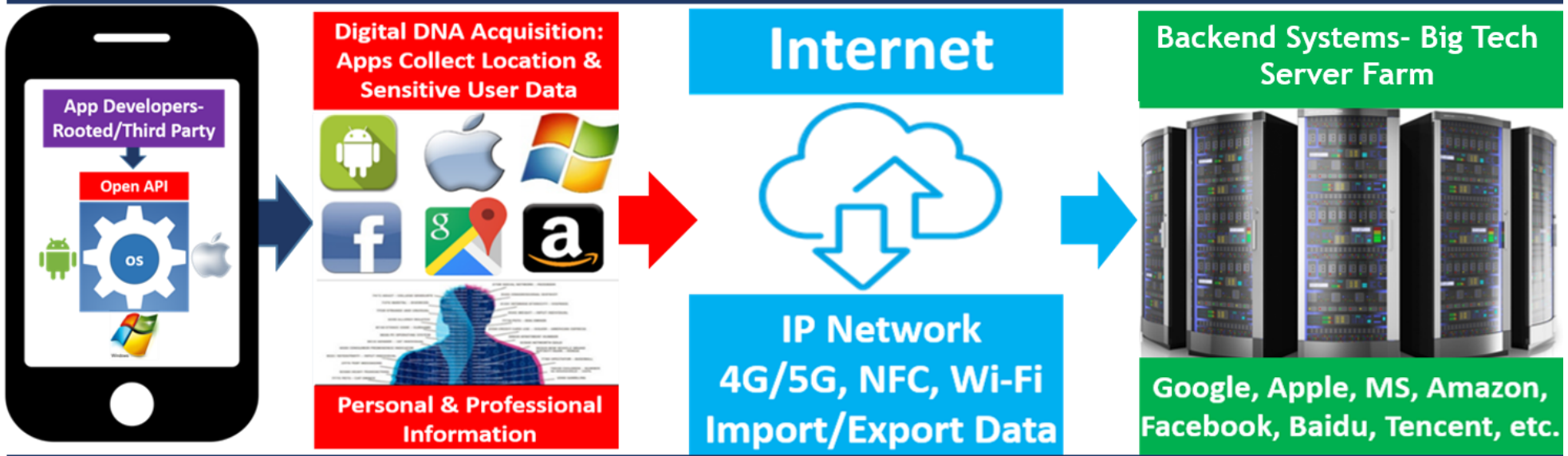
Samsung KNOX android APP- Interactive Application Permission Command String Analysis. Samsung Galaxy Note- App Cannot be Disabled by User



Question- Why is Google Enabling Facebook Access to Surveillance and Sensitive User Data via the Installed Samsung KNOX Application?

My Smart Privacy™
Privacy & Data Security

Android OS (Google), Apple iOS, & Microsoft Windows OS
Open API Flow Chart- Importing and Exporting Personal & Professional Information!



Connected Technology: Smartphones, Tablet PCs, Connected Products, IoT/IIoT Devices, Voice Automated Assistants, Vehicles, TVs, Appliances, and PCs

Due to Open API Architecture All Products Cannot be Privatized or Secured!

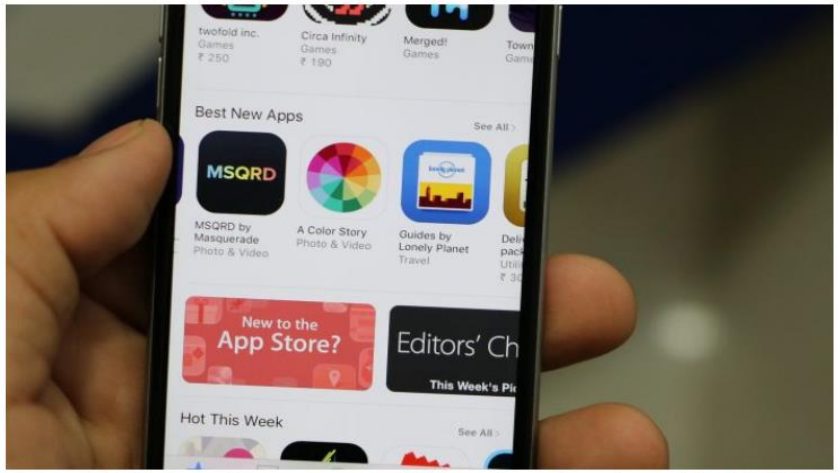
Confidential & Protected Environments

Is the Use of Smartphones Legal?

Smartphones show the ride-hailing apps Uber Technology Ltd., left, and Didi Chuxing at a residential compound in Beijing, on Aug. 1, 2016. (AP Photo/Andy Wong)

Business Users of Smartphones May Be Breaking the Law

Rex M. Lee



File photo of the Apple app store. Some apps come pre-installed on smartphones and cannot be controlled or uninstalled. The rest must compete via app stores such as those of Google and Apple. (ParampreetChanana/pixabay.com)

Telecom and Tech Giant Conflict of Interest and Competition Violations: Part 1

Rex M. Lee

My Smart Privacy™
Privacy & Data Security

Confidential and Protected Environments!

The Defense Industry, Critical Infrastructure, & Enterprise Business

A Confidential and Protected Environment is governed by confidentiality agreements, NDAs, industry & federal cyber security standards, federal information processing standards ("FIPS") and confidentiality laws that govern medical information, client attorney privilege and classified information.

My Smart Privacy™
Privacy & Data Security

Cybersecurity Threats at The Strategic Level
C-Suite Executive & Board

The Resurgence of Great Power Competition- China, Russia, & Others
Google, Apple, & Microsoft Distribute Surveillance & Data Mining Tech Developed by Chinese & Russian Tech Companies

A man walks past an advertisement for the WeChat social media platform, owned by China's Tencent, at Hong Kong International Airport on Aug. 21, 2017. RICHARD A. BROOKS/AFP/Getty Images

Google, Apple, and Microsoft Distribute Chinese Surveillance Technology

Rex M. Lee

My Smart Privacy™ Privacy & Data Security

BLACKOPS PARTNERS

www.MySmartPrivacy.com

The Resurgence of Great Power Competition- China & Russia

Cybersecurity, Privacy, & National Security Threats

"Russia and China are competitors to the United States and both nations are looking to overturn the current rules-based international order…both trying to assert greater influence on the world stage"- Chairman Joints Chiefs of Staff, General Joseph F. Dunford, CNN 03.2019.

What is at Stake?, Economic Dominance by America, National Security, Cybersecurity, Personal/Professional Privacy, and Billions in Stolen American Intellectual Property ("IP"):

"A change to the world order is underway, the ground has shifted due to the threat of Great Power Competition, Unprecedented Risk, and Asymmetrical Hybrid Warfare"- Casey Fleming, CEO, BLACKOPS Partners, Washington D.C.

Secretary of State Mike Pompeo Confirms Threats from China & Russia at CERAWeek 2019 and CBS News: "Threats Posed by Great Power Competition from Russia and Chine (March CERAWeek 2019)…..Espionage & Theft of Billions of Dollars Worth of American Intellectual Property per Year (CBS This Morning, April 2019)".

How to Respond!:

- Great Power Competition is an invisible top threat to every company that must be addressed immediately at the strategic layer by all C-levels and Board
- Your response begins with Awareness, Training, then Focus!

My Smart Privacy™
Privacy & Data Security

BLACKOPS PARTNERS

MATURE NATION-STATE GREAT POWER COMPETITION

UNPRECEDENTED RISK / ASYMMETRICAL HYBRID WARFARE

Cybersecurity is No Longer just a Threat at the Tactical Level (IT)!

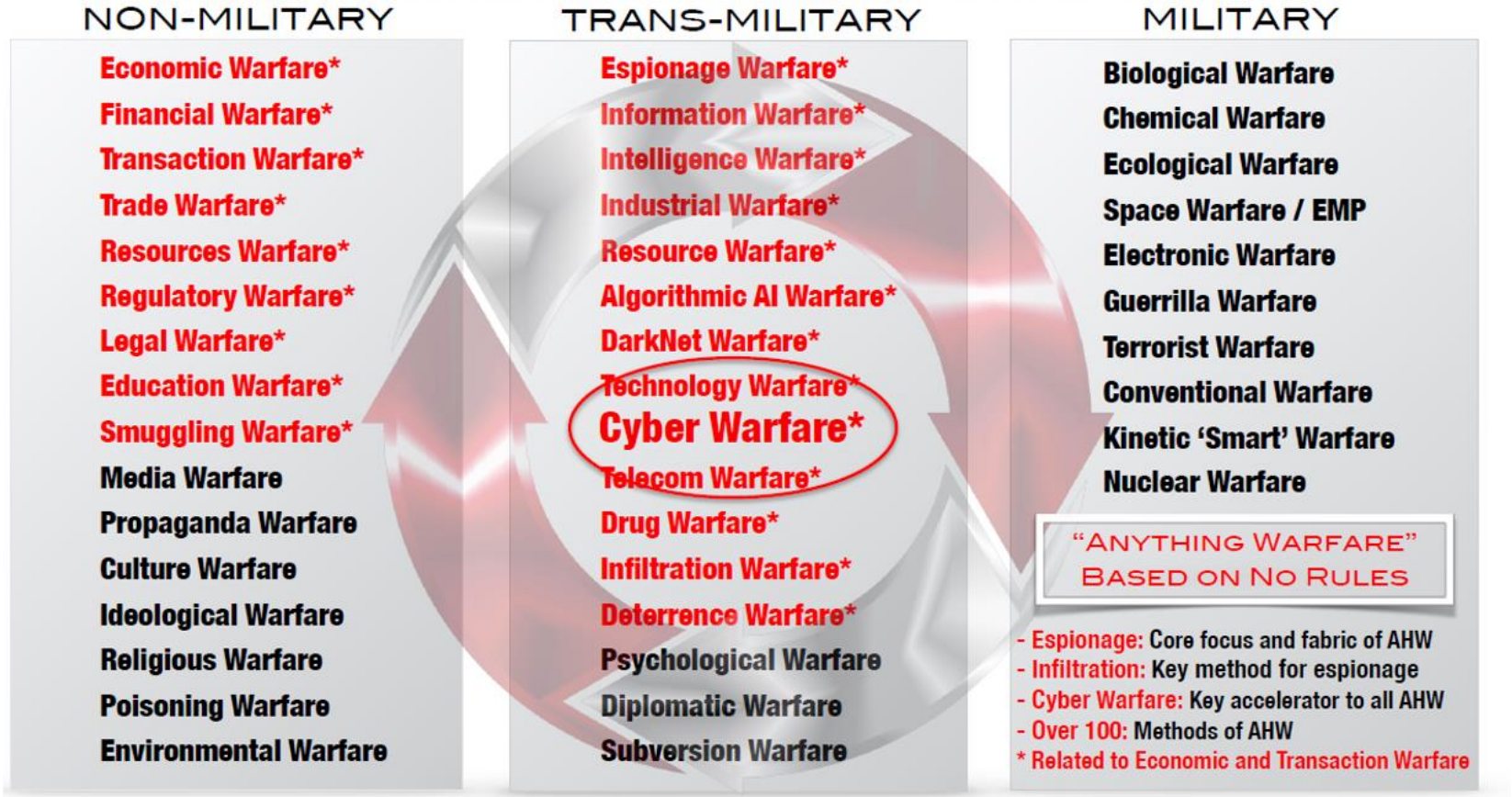
Cybersecurity is a Also a Threat to the Strategic Level- C-Suite & Board!

MATURE NATION-STATE GREAT POWER COMPETITION

UNPRECEDENTED RISK / ASYMMETRICAL HYBRID WARFARE

THE MODERN BATTLEFIELD IS EVERYWHERE

UNRESTRICTED WARFARE TARGETING ALL ORGANIZATIONS AND CIVILIANS



BLACKOPS. PARTNERS

Cyber, Tech, & Telecom Threats
Legal Malware- Intrusive Google, Apple, & Microsoft Apps

Trans-Military Threats: Cyber, Tech, and Telecom Warfare

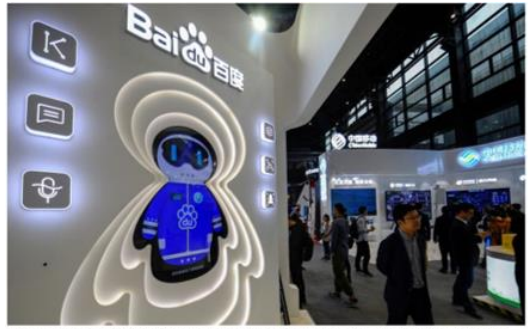
Non-Military Threats: Trade-Warfare

Legal Malware: Intrusive Google, Apple, & Microsoft Apps Developed by Russian & Chinese Companies such as Baidu, Tencent, & Prisma Labes

BLACKOPS PARTNERS

Best Practices and Polices!

Smartphones, Tablet PCs, Connected Products, PCs, & B.Y.D.D. Programs



A man walks past a Baidu booth on Nov. 6, 2018, at the Light of Internet Expo ahead of the fifth World Internet Conference in Wuzhen in China's eastern Zhejiang province. (STR/AFP/Getty Images)

Google Distributes Surveillance Technology Developed by Chinese Company

Rex M. Lee

People walk by as the social network Facebook opens a pop-up kiosk for one day in Bryant Park in New York, Dec. 13, 2018, where it fields questions about its data-sharing practices and teach users how to understand its new privacy controls. (TIMOTHY A. CLARY/AFP/Getty Images)

Smartphone App Users Are Data-Mined Even When Not Using the Apps

Rex M. Lee

This illustration picture taken on April 20, 2018 in Paris shows apps for Google, Amazon, Facebook, Apple (GAFA) and the reflexion of a binary code displayed on a tablet screen. (Lionel Bonaventure/AFP/Getty Images)

Telecom and Tech Giant Conflict of Interest and Competition Violations: Part 2

Rex M. Lee

Children play video games on smartphones while attending a public event on Sept. 22, 2012 in Ruesselsheim, Germany. (Sean Gallup/Getty Images)

The Need for an Electronic Bill of Rights: Part 2

Rex M. Lee

My Smart Privacy™
Privacy & Data Security

Best Practices & Policies

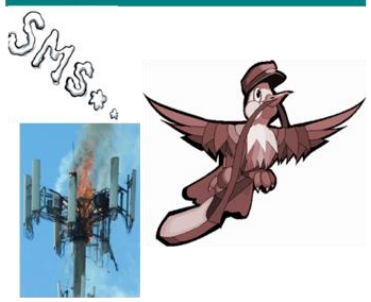
- Private Networks & Licensed Spectrum
  - Radio access networks (“RANs”)/field area networks (“FANs”), LTE wireless infrastructure as a service (“W-IaaS”), Nokia & AT&T private LTE network, & Licensed spectrum
- Device Solutions
  - Feature phone and/or flip phone (non-app driven/no GPS/no data services)
    - Note that Google has cut deals with numerous OEMs to support the OS on flip phones
  - Proprietary devices supported on LMR, RAN, and FAN
    - Note some LMR OEMs are adopting the android OS to support two way radios- Stay Away!
  - Preconfigure smartphones, tablet PCs, Connected Products, IoT/IIoT Devices, LMR Devices, & PCs prior to activation & use
- Do Terms of Use & Preinstalled App Analysis & Demand Transparency
  - Stay away from “Free Anything”- Free stuff is paid for by personal and professional information
  - Read your Terms of Use coupled with SLAs and terms of use (products, network, ELUAs, cloud storage, etc.)
  - Analyze pre-installed apps, widgets, etc.. on connected devices
  - Do not download or purchase any 3rd-party apps/do not allow employees to download 3rd-party apps
  - Do not allow any vendors to communicate official business on consumer grade connected technology
  - Do not adopt a bring your own device (“B.Y.O.D.”) program
    - Terminate any existing B.Y.O.D. program
  - Set up an appointment with your telecom provider and discuss privacy and cyber security issues associated with connected technology. Demand transparency, ask questions, file complaints, and litigate if necessary!
- Electronic Bill of Rights- Elected Officials, Government Officials, and Consumers Need to Take Action!

Cybersecurity In 2019

The "Unconnected Network!"

Secure Voice & Data Network

Encrypted Wireless Networks



Cyber Security- Encrypted Data Protection & Firewall

Secure Redundant Cloud Data Storage

My Smart Privacy™
Privacy & Data Security

What Year Is It 2019 or 1984?

My Smart Privacy™
Privacy & Data Security

According to Google it is 1984

"……. We know where you are. We know where you've been. We can more or less guess what you're thinking about"- Eric Schmidt-Google

Rex M. Lee
www.MySmartPrivacy.Com

My Smart Privacy™
Privacy & Data Security

BLACKOPS PARTNERS