

Data Privacy

Our Latest Research



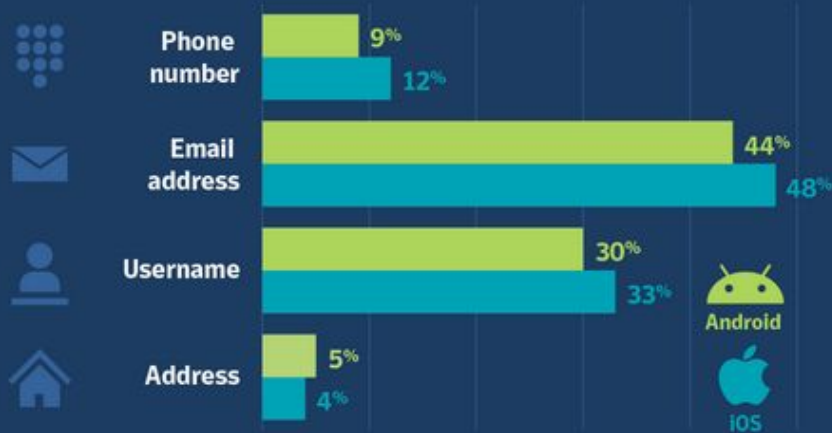
Aaron Dawson, Shengjia He, Tom Lancaster, & Danniell Sotelo

App Collection

- Apps have access to IMEI and MAC address
- Between apps, what is collected depends on mobile OS and App Store
- Social Media logins on app acts as third-parties - Social Media Integration
- Android apps using Graph API use certificate pinning -It's a security precaution that helps prevent attackers intercepting supposedly secure communications
- Risky Permissions - user's location, contacts, messages, phone logs, camera, calendar
- Not all risky permissions are bad, despite the name

Gillian Cleary. 2018. Mobile Privacy: What Do your Apps Know About You? (Aug 2018)
Retrieved July 28, 2019 from
<https://www.symantec.com/threat-intelligence/mobile-privacy-apps>

Personally identifiable information (PII) shared with apps



Risky permissions

Percentage of apps that request risky permissions by operating system



Q: What are “risky permissions?”

A: Permissions where the app requests data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps

Risky permissions breakdown



Privacy checklist



Just because an app is requesting personal information or risky device permissions, it doesn't mean it is up to no good. Most apps will have a good reason for doing so. For example, a fitness tracking app may need to track your location in order to work properly. Before you install an app, ask a few questions:

01 Do I know what information and permissions an app is requesting?

02 Am I comfortable sharing personal information with this app developer?

03 Does the app really need the device permissions it is requesting?

Gillian Cleary. 2018. Mobile Privacy: What Do your Apps Know About You? (Aug 2018)
Retrieved July 28, 2019 from
<https://www.symantec.com/threat-intelligence/mobile-privacy-apps>

Browser vs App

Which is better protecting your data? Well, it depends!

- Locations and names leaks more often on browsers, passwords leaks
- Apps leak specific device information and unique identifiers
- Websites contact more domains (advertisers)
- Education and Weather apps contact more domains while Entertainment apps contact the least
- The types of PII leaked by Web- and app-based versions of the same service share nothing in common more than half of the time
- <https://recon.meddle.mobi/appvsweb/>

David Choffnes. 2016. Should You Use The App For That? Comparing the Privacy Implications of App- and Web-based Online Service (2016)

<https://david.choffnes.com/pubs/AppVsWeb-IMC16.pdf>

A&A Domain	# of Services:			Avg. Leaks:		Leaked Identifiers:		
	App	∩	Web	App	Web	App	∩	Web
amobee	1	1	1	517.0	314.0	3	2	2
moatads	9	7	12	61.4	0.2	1	1	1
vrvm	2	0	0	136.0	0.0	3	0	0
google-analytics	35	32	41	1.8	2.5	1	1	2
groceryserver	1	1	1	154.0	0.0	1	0	0
serving-sys	10	4	6	15.3	0.0	1	0	0
facebook	38	36	41	3.7	0.3	2	0	1
googlesyndication	16	14	23	7.0	0.8	1	1	1
thebrighttag	4	2	4	29.5	0.0	2	0	0
tiqcdn	5	5	9	16.0	3.1	1	1	1
marinsm	1	1	3	96.0	1.0	1	0	1
criteo	7	6	22	8.9	1.1	2	1	2
2mdn	14	9	17	5.8	0.0	1	0	0
monetate	1	1	2	74.0	0.0	1	0	0
247realmedia	1	1	2	48.0	12.0	1	0	1
krxd	7	6	13	8.3	0.0	3	0	0
doubleverify	3	2	7	19.3	0.0	1	0	0
cloudinary	1	1	1	0.0	58.0	0	0	1
webtrends	1	1	1	56.0	0.0	1	0	0
liftoff	1	0	0	54.0	0.0	2	0	0

Table 2: Top-20 A&A domains, sorted by total leaks.

David Choffnes. 2016. Should You Use The App For That? Comparing the Privacy Implications of App- and Web-based Online Service (2016)

<https://david.choffnes.com/pubs/AppVsWeb-IMC16.pdf>

PII	# of Services:			Avg. Leaks:		Domains Leaked To:		
	App	\cap	Web	App	Web	App	\cap	Web
Location	31	21	26	356.0	295.2	84	37	76
Name	9	8	16	77.1	138.2	11	7	26
Unique ID	39	0	0	40.0	0.0	64	0	0
Username	3	1	4	23.0	100.2	4	2	9
Gender	4	1	8	3.0	25.0	4	1	11
Phone #	3	1	2	12.7	60.5	3	1	2
Email	10	2	7	2.3	17.6	10	1	7
Device Name	15	0	0	2.7	0.0	13	0	0
Password	3	1	2	3.0	2.0	3	1	1
Birthday	1	0	1	1.0	3.0	1	0	2

Table 3: PII, sorted by total leaks.

David Choffnes. 2016. Should You Use The App For That? Comparing the Privacy Implications of App- and Web-based Online Service (2016)

<https://david.choffnes.com/pubs/AppVsWeb-IMC16.pdf>



Retailer	Uses Face Recognition?
Wal-Mart Stores	Refused to answer
Costco	Refused to answer
Target	Refused to answer
McDonald's	Refused to answer
Lowe's Companies	YES
Best Buy	Refused to answer

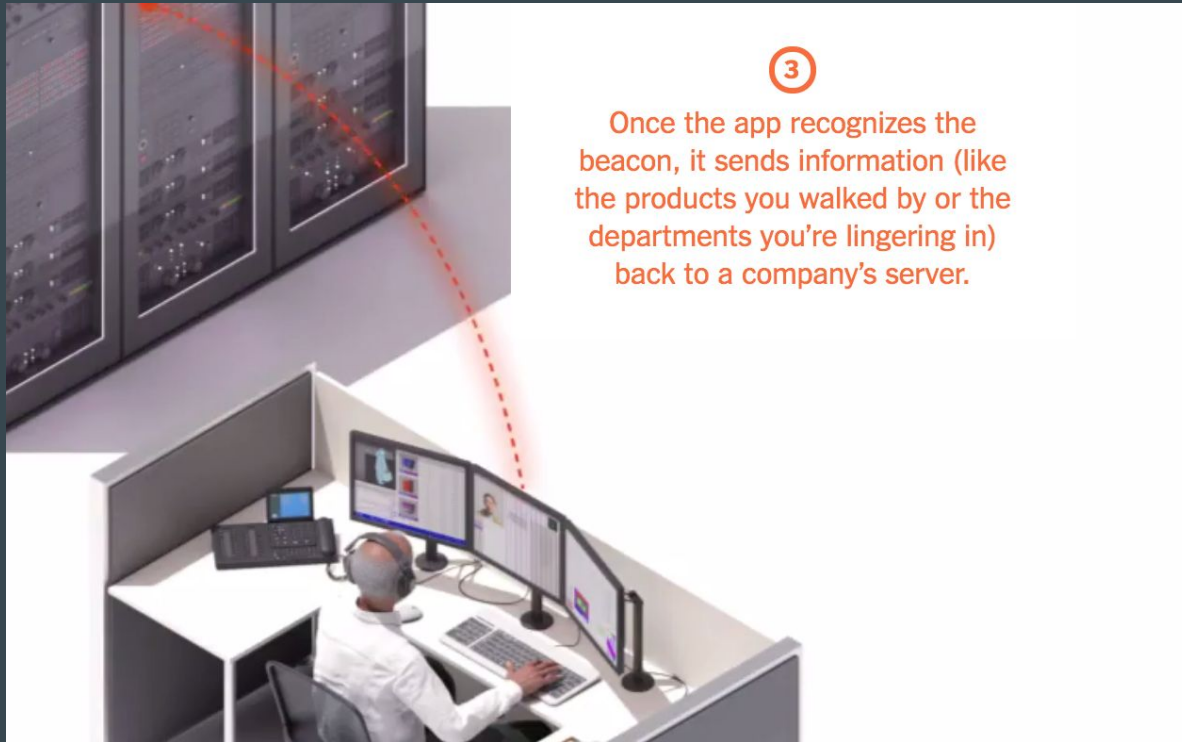
Source: Bitar, Jenna, and Jay Stanley. "Are Stores You shop at Secretly Using Face Recognition on You?" *American Civil Liberties Union*, 26 Mar. 2018, www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face.



Source: Kwet, Michael, "In Stores, Secret Bluetooth Surveillance Tracks Your Every Move." *The New York Times*, The New York Times, 14 June 2019, www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.



Source: Kwet, Michael, "In Stores, Secret Bluetooth Surveillance Tracks Your Every Move." *The New York Times*, The New York Times, 14 June 2019, www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.



3

Once the app recognizes the beacon, it sends information (like the products you walked by or the departments you're lingering in) back to a company's server.

Source: Kwet, Michael, "In Stores, Secret Bluetooth Surveillance Tracks Your Every Move." *The New York Times*, The New York Times, 14 June 2019, www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.



4

Foot traffic information can reveal personal details such as your income and exercise habits. When paired with other information about you, companies can build a rich profile of who you are, where you are, and what you buy — all without your knowledge.

5

The app can be prompted to display ads for products you seem likely to buy. It can send you a coupon after you leave, urging you to come back — a practice called “retargeting.”

Source: Kwet, Michael, “In Stores, Secret Bluetooth Surveillance Tracks Your Every Move.” *The New York Times*, The New York Times, 14 June 2019, www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

How much is your data worth?

Depends on which side your on - Customer vs. Business



How much is your data worth? - Customer Side

- Facebook - FTC fine = \$5 billion
 - 200 million affected FB users
 - \$25 per person \approx Dinner Entree
- Equifax - FTC fine = \$700 million
 - 147 million affected users
 - \$5 per person \approx Double Chalupa Box from Taco Bell
- Amazon Prime Day Blitz
 - Agree to let Amazon Assistant follow you on Internet
 - \$10 off purchase of \$50 \approx Any pizza from Pizza Hut



How much is your data worth? - Business Side

- Facebook
 - Ad revenues 2019 Q2 = \$16.9 billion revenue
 - \$2 billion profit
 - Continue to sell our data
- Equifax
 - 2019 Q2 = \$880 million
 - Continue to sell our data
- Amazon
 - Ad Revenue 2019 Q2 - \$2 billion
 - Mastered data analytics through website
 - Continue to maximize sales from users



Financial Calculator - Volunteer?

<https://ig.ft.com/how-much-is-your-personal-data-worth/>

How much is your data worth? - Financial Calculator

Group Member	Data's Value
Aaron	\$0.0137
Danniel	\$0.363
Shengjia	\$0.1763
Tom	\$0.363

Sources: <https://ig.ft.com/how-much-is-your-personal-data-worth/>

Ramifications - Fortnite Champion “Swatted”

- 16-year-old Fortnite Champion Kyle “Bugha” Giersdorf “swatted” during live Twitch stream
- **Negative**
 - “Swatted” = Deceiving emergency service into sending a SWAT team
- **Positive**
 - Twitch video gaming streaming service
 - Highest Earner - Ninja - \$560k/month



Questions?