Shawn Kenney

Designing for Privacy

Guide Introduction

This presentation was initially given to the (defunct) Cleveland Chapter of UXPA in September of 2015 by myself and IBM colleague Brian Anderson.

The information in this presentation was based on research from numerous sources and conferences with original research being noted where applicable. Where available, research stats have been updated using updated sources.

Defining Privacy

Defining Privacy

“Broadly speaking, privacy is the right to be left alone, or freedom from interference or intrusion.

“***Information privacy*** is the right to have some control over how your personal information is collected and used.”

-privacyassociation.org

When we think privacy, what do we think of?

Privacy Policies

The legal statements companies abide by when accessing and storing our personal information and their intentions with it.

Data Encryption

The technical protection at the data level that prevents unauthorized individuals from deciphering our personal information.

Asset Protection

The physical hardware or software that protects companies and ourselves, keeping intruders from gaining access to our information.

Self Determination

The right for myself as an individual to decide who gets access to my information and how they may use it.

“Big Brother”

Entities more powerful than any individual who have the ability to use data to cause harm or make me uncomfortable.

Privacy is all of these things

When we think about privacy, we think about all of these things. How we think about privacy, and which aspects of privacy we consider at any given moment depends on the individual and their circumstance.

We are privacy's weakest link

In August 2015 I conducted an informal, ad-hoc, non-scientific, unpublished, non-peer reviewed survey of Facebook friends.

Q1: Would you consider it a privacy breach if your name, address, phone number and account information was published to an unaffiliated third party by a company or service you utilized?

A1: 100% Yes

Q2: Same question, but this time it was due to your using the wrong e-mail address (either deliberately or accidentally).

A2: 100% No

They would not consider it a privacy breach, even if the wrong e-mail address was put in by accident.

What's the problem with this scenario?

Personal responsibility over ones privacy is fine, but the user is still vulnerable to having their privacy compromised even if they unknowingly contributed to the breach.

While this may or may not be an issue for the company involved from a legal perspective, allowing this as a designer would violate the usability heuristics of error prevention and helping users recognize, diagnose, and recover from errors.

- "10 Usability Heuristics", Nielsen Norman Group

Why would someone use the wrong e-mail?

•They fat finger it — it happens!

•They don't feel an e-mail account should be necessary to utilize the service (ex: Redbox).

•They want privacy; they may not want to be contacted or spammed, and may a service that provides a temporary, time bombed e-mail address that can't be traced back to them (examples: mailinator, fakemailgenerator.com)

Since 2015, two-factor authentication has become a best practice when creating online accounts to help verify the account creator owns the address.

Deanonymization from 4 pieces of data

In 2014, a group of M.I.T. grad students analyzed 3 months worth of “anonymized” credit card data from 1.1 million people used at over 10,000 stores.

The dataset contained the date of each transaction, amount charged and name of the store.

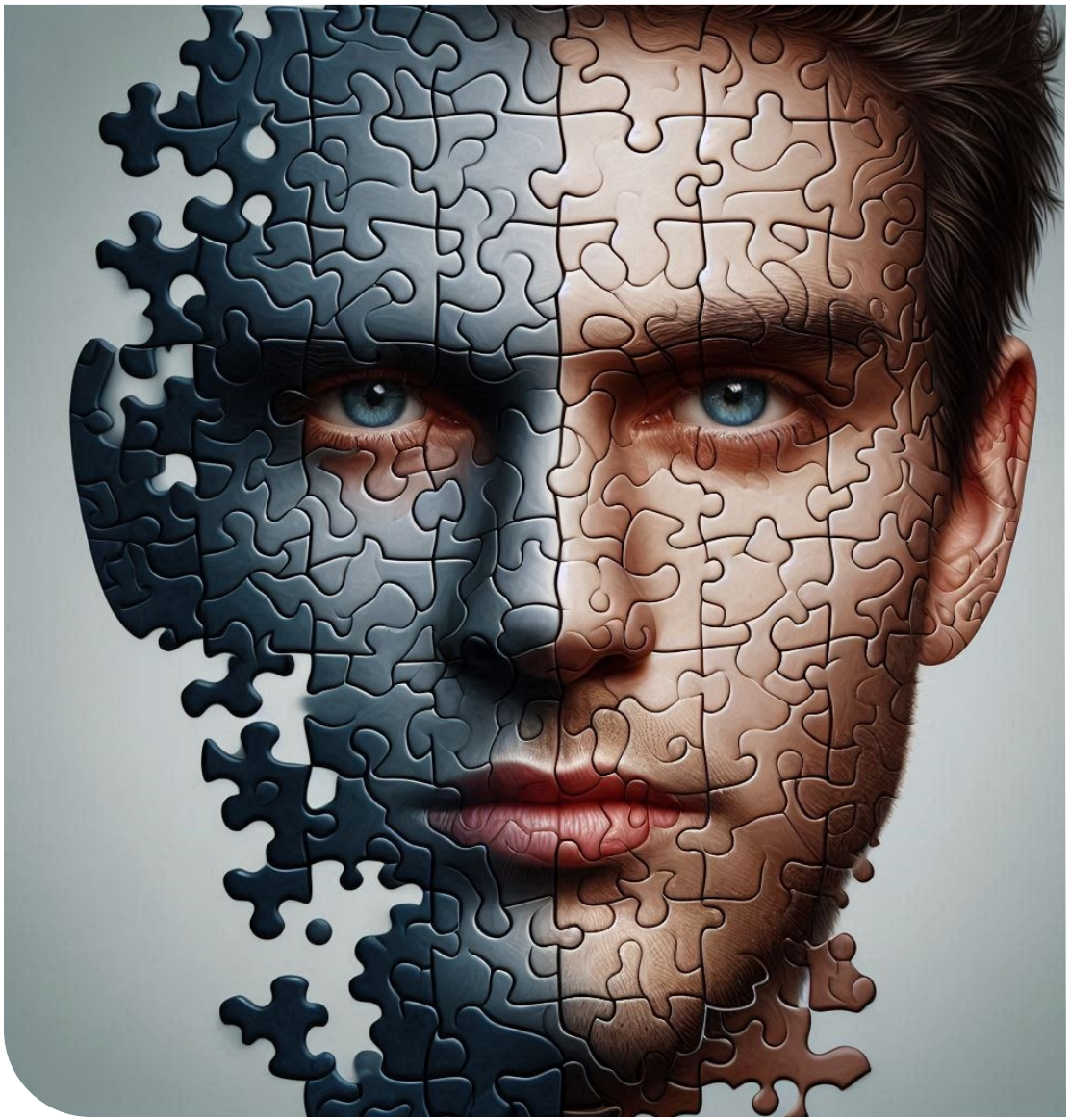
The uniqueness of the records, combined with publicly available social media content allowed the researches to reidentify 90% of the records by the persons name.

- “With a Few Bits of Data, Researchers Identify ‘Anonymous’ People” New York Times

A decade later, this is still an issue

For good and bad...

- In April 2024, it was reported that German authorities were able to deanonymize users of the Tor web browser in order to make an arrest in a child abuse case.
- In 2023, Russian authorities were announced as having technology that would allow them to deanonymize users of Telegram to control unfavorable information about the government.
- In 2022, researchers showed that Bitcoin traders could be deanonymized, despite claims from Bitcoin touting their anonymous structure.



Ethical Design Considerations

What is the scale of data being collected?

- IoT Analytics estimates 18.8 billion wirelessly connected devices exist in 2024.
- S&P Global states a connected car can generate 25GB of data in just 1 hour.
- in 2015 IBM predicted we'd have 4 times as many pieces of data than grains of sand on earth by 2020.
  - In 2019 the World Economic Forum's predicted it would be 6 times as many by 2020.
  - By the end of 2024, Statista estimates this will increase to 21 times as many.

Data as a natural resource

- Data is the only resource that is increasing in quantity, not decreasing.
- It has the ability to be utilized repeatedly, and remain as valuable tomorrow as it is today.
- Just like a natural resource it needs to be refined. As technologies like AI and analytics improves, the value of data increases.
- It’s the single most valuable resource businesses have.
- Estimates from IBM and Forrester suggest between 70% and 80% of this data goes unanalyzed.

What is our role as designers?

Should we have a say in the types of user data a business collects?

How ethical should we be? Should we view ourselves as the ethics police in our organizations?

How can we position research to inform when a business need may cross a privacy line?

As designers, are we even part of the conversation around data and it's potential impact on users?

Ethical done right: home health care

- Home wired to monitor an elderly woman who lived alone by her son, who was notified of deviations in her behavior.
- Was the woman worried about her privacy being invaded? No:
  - “I felt more connected to my son. If something changed he would call to see how I was doing”
- But, she still wanted to maintain, such as when her “significant other” was over.

- Beth Mynatt, Georgia Tech

Ethical done wrong: e-commerce

- Target sends coupons to a teenage girl based on her shopping habits.
- The coupons begin to feature products that reflect the needs of a pregnant woman.
- Father finds coupons and is upset that Target would send these to a minor.
- Father contacts Target, then learns his daughter is pregnant.

- “How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did”, Forbes 2012

When technology becomes creepy

Google Glass was seen as creepy in 2013. A decade after Meta is trying their hand at glasses. But what made them creepy then and now?

- It takes the power out of our hands and puts it into the wearers
  - Is it on?
  - Is it pointed at me?
  - Is it/has it been recording me?

These same concerns still exist almost a decade later with Meta/RayBan's latest attempt, running up against regulators

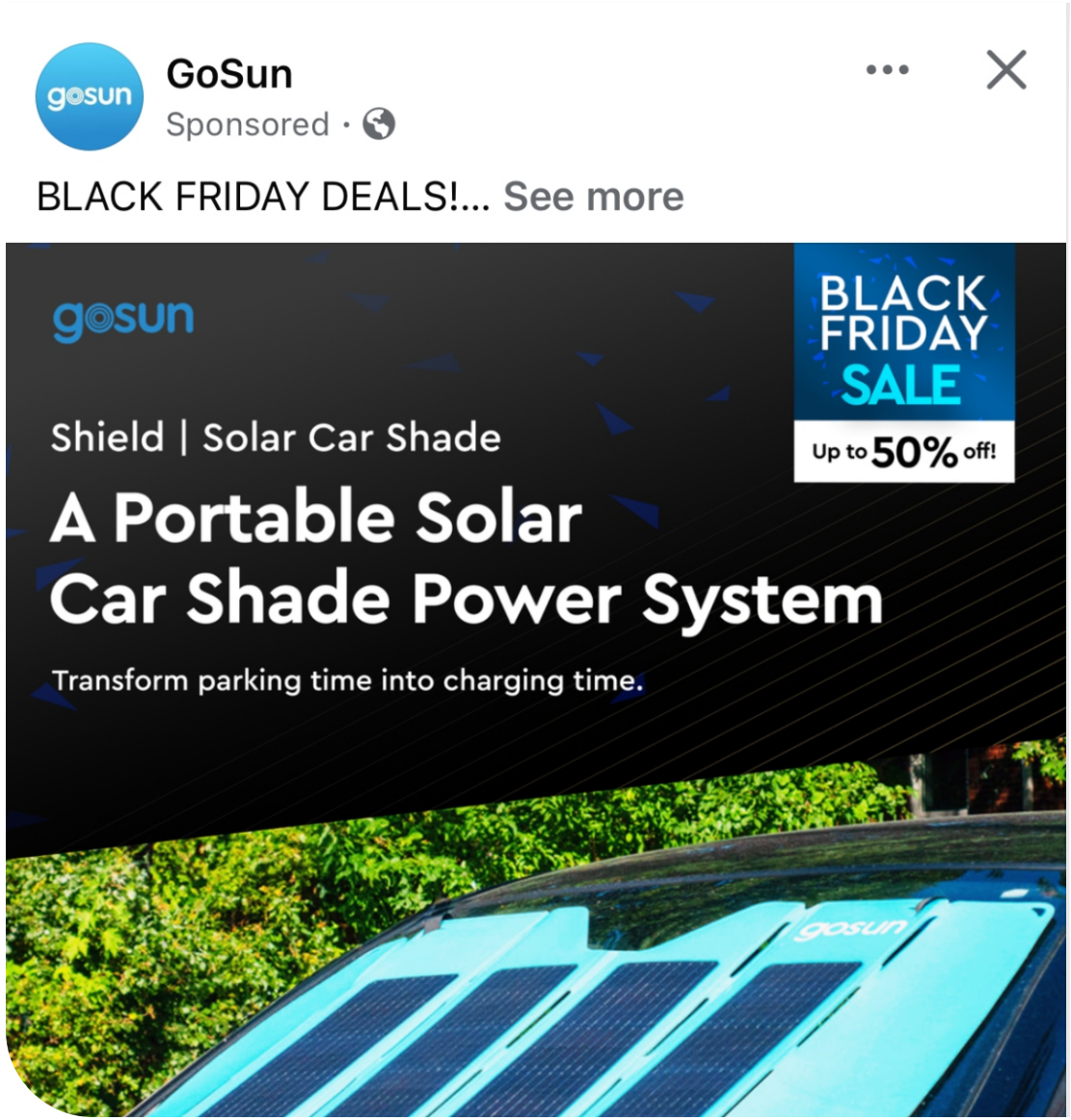
- "Why Google Glass is Creepy", American Scientific

- "Meta's Smart Glasses Ignore Why Google Glass Failed", The Daily Beast

Ethical perceptions can be generational

In 2013, a survey showed that 75% of web users noticed that ads were targeting them as they moved between websites. 55% of respondents were very or somewhat concerned that retailers could show them ads after they visit a website.

According to statista, in 2022 surveys showed that 81% of Gen Z respondents liked personalized ads, as did 57% of millennials. Baby boomers showed the least support for personalized ads at a little over 40%.



Ethical usage must match user expectations

Users recognize situations where they may want data to be collected, such as health monitoring devices which have a benefit to the user when analyzed.

Using the data in a way that the user would not expect may make them uncomfortable, or place them in direct harm, such as exposing that a minor may be pregnant before she's ready to disclose it.

As designers can we use personas and "extreme users" to identify and avoid these situations in advance?

When asked in a Carnegie Mellon survey, 95% of respondents were surprised that Brightest Flashlight iPhone ap) gathered geolocation data, but "almost no one" was surprised that Google Maps tracked personal location.

It's understood that mapping software would need you location, but not easily understood why a flashlight would.

- "A Shock in the Dark: Flashlight App Tracks Your Location", New York Times

Privacy calculus theory

Individuals often will invent reasonable explanations for conditions that initially appear to them to be unreasonable, such as a flashlight or dictionary app that requests location data.

Once they have rationalized this and weighed the perceived risk against the value, they can continue moving forward without conflict. This concept is called “privacy calculus theory”.

- Theory Hub, Privacy Calculus Theory

Technology and risks continue to advance

With the introduction of generative AI systems, we're now willingly entering personal and business data into systems which can then be used to train the system and generate new content for others or be exposed through a security breach.

Additionally, some of these systems have identified as having the ability to screen capture users displays and potentially monitor users behavior, potentially in the workplace.

- "AI Is Your Coworker Now. Can You Trust It?", Wired June 4, 2024

Who do we trust with privacy?

76% of survey respondents in a 2013 TRUSTe survey say themselves. Social networks like Facebook received just 1% of the vote.

In 2022, Varonis looked to identify which institutions Americans felt would most likey protect their personal information. Credit card companies scored the highest at 35%, while the federal government followed at 31%. Social media sites came in last at 5%.

- “US Web Users Concerned About Privacy, but Hold Themselves Accountable”, eMarketer

- “Americans and Privacy Concerns: Who Do We Trust?”, Varonis

Do users understand privacy?

In 2019, Pew Research found that 36% of adults never read a privacy policy and another 38% sometimes read privacy policies.

Being willing to read them however is only half the battle. Most are written at a 10th grade to college reading level, while most American's read at a 7-8th grade level.

-"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information", Pew Research

- "It's Not You; Privacy Policies are Difficult to Read", Common Sense Education

Best Practices for Privacy Design

Should we be collecting data?

Yes, with a focus on building trust.

Building trust with those you are collecting data from should be a primary design decision.

The key is putting the users trust in the forefront of the design decision making process:

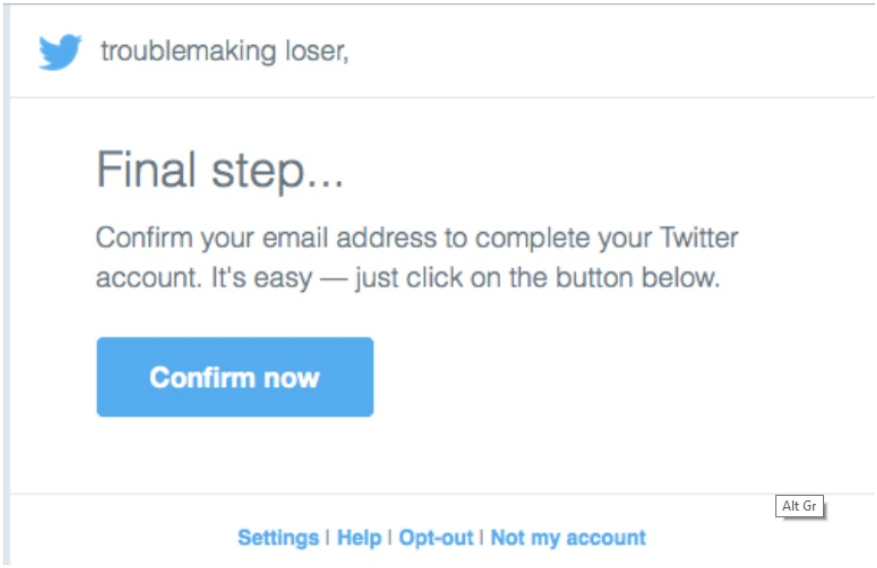
- Understand your users expectations to what data you need.
- Understand the value each piece of collected data will provide the user.
- Understand what is important to them in terms of protecting their privacy.
- Be transparent in communicating the need to your users.

Validate your users up front

Do your best to make sure they at least own their own unique identifier (e-mail address, customer ID).

Don’t permit access to your services until it has been confirmed.

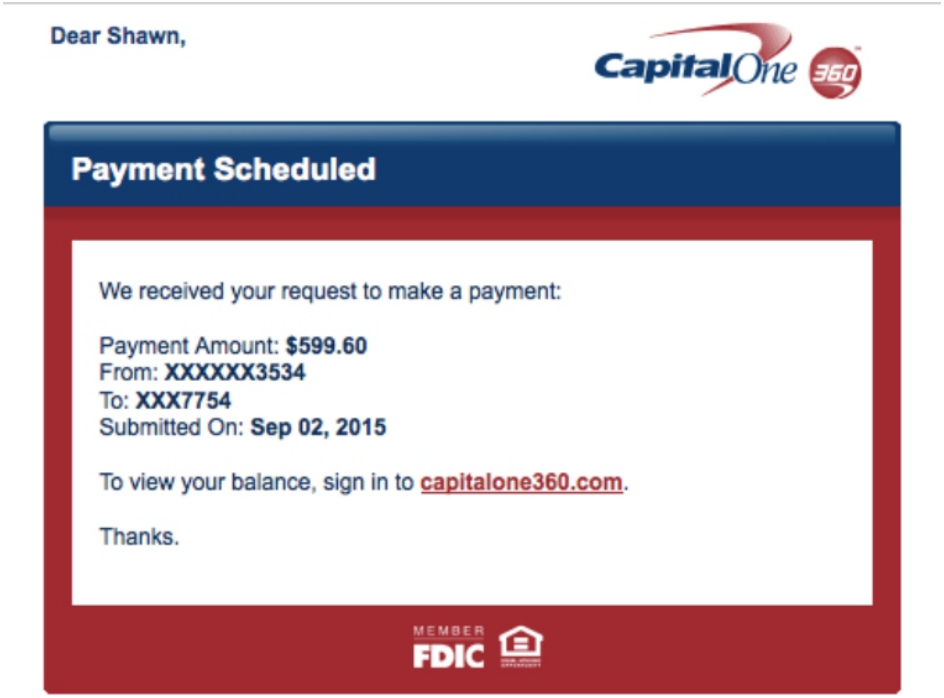
Twitter would ask users to confirm their account before it was activated, and gave the owner of the e-mail address the chance to close the account in the event someone attempted to create one with their e-mail address.



Only disclose the bare minimum

Only disclose the bare minimum, even to the intended user.

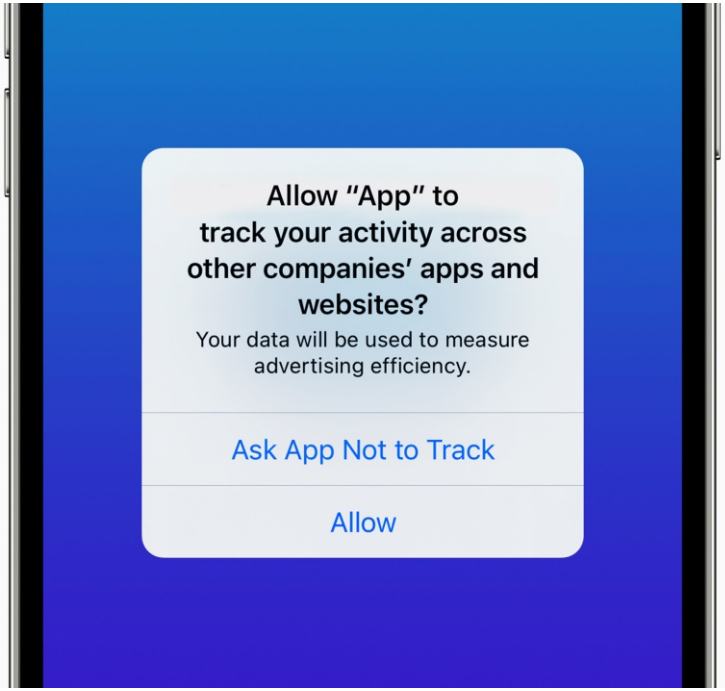
Should a users personal security become breached, or should they unintentionally breach their own personal security, don't compound the problem by exposing to them information they should already know even as a courtesy, especially if it can be used against them later on.



Be real about users data

Understand the data you wish to collect about your users, and the data they would expect to be collected about themselves. Identify potential gaps in expectations and be ready to communicate the value the user would receive when there is a gap.

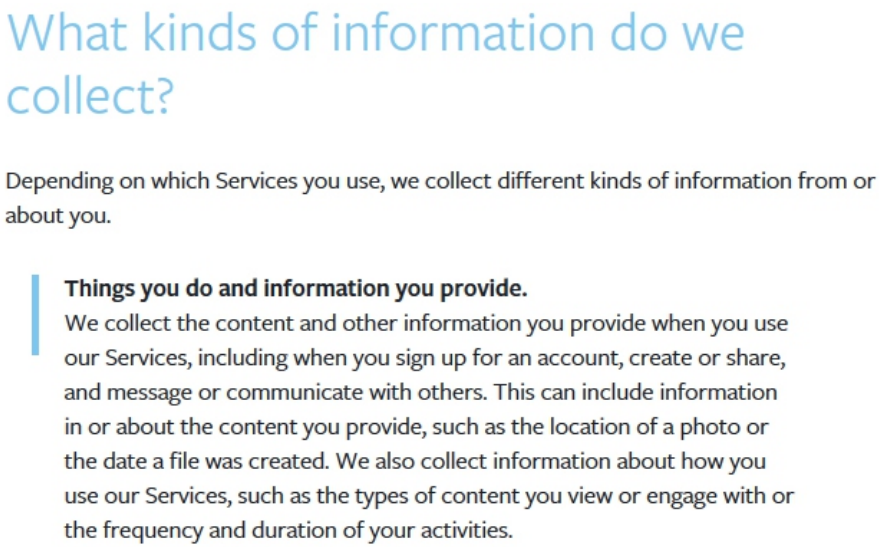
Revealing that you have more information about them then they would expect to will introduce a level of creepiness and unease to the relationship, especially if a security incident occurs.



Ensure privacy policies are human readable

Most people are not lawyers, and privacy policies are written to protect the company, not the user.

- Write privacy information in plain language targeted for a general audience.
- Provide links back to the full legal privacy policy for transparency.
- Make privacy information accessible from within the app during moments where data is being collected.



What kinds of information do we collect?

Depending on which Services you use, we collect different kinds of information from or about you.

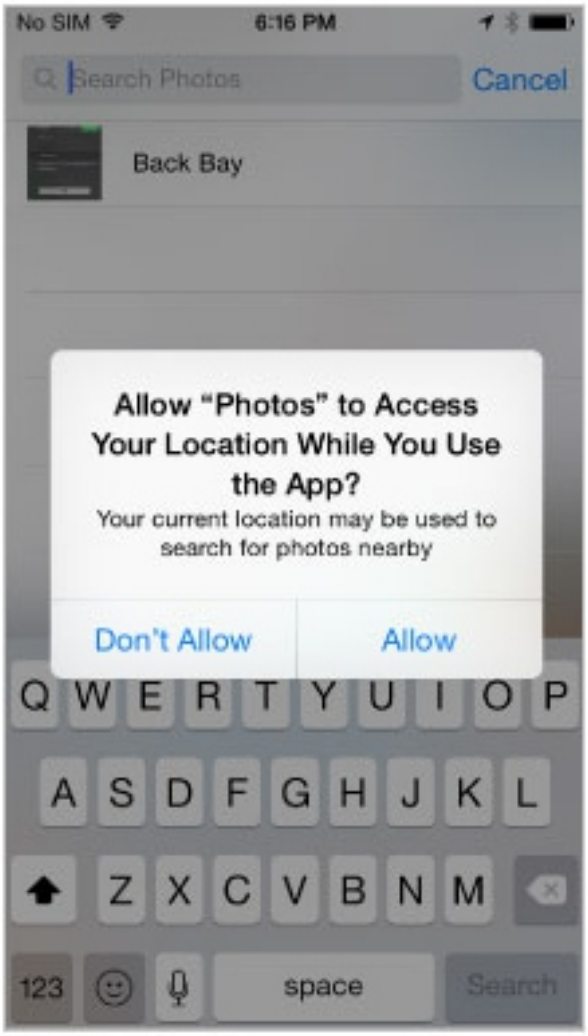
> **Things you do and information you provide.**
> We collect the content and other information you provide when you use our Services, including when you sign up for an account, create or share, and message or communicate with others. This can include information in or about the content you provide, such as the location of a photo or the date a file was created. We also collect information about how you use our Services, such as the types of content you view or engage with or the frequency and duration of your activities.

Simplify privacy settings for users

Create default privacy settings that match identified expectations.

Provide settings for those items outside of the expectations along with explanations why having the user enable them would be useful to the service provider.

Prompt the user in real time, and in context to change a setting when they are accessing a feature their privacy settings don't allow for. Don't ask for a lot of personal data up front if they won't benefit from it right away.

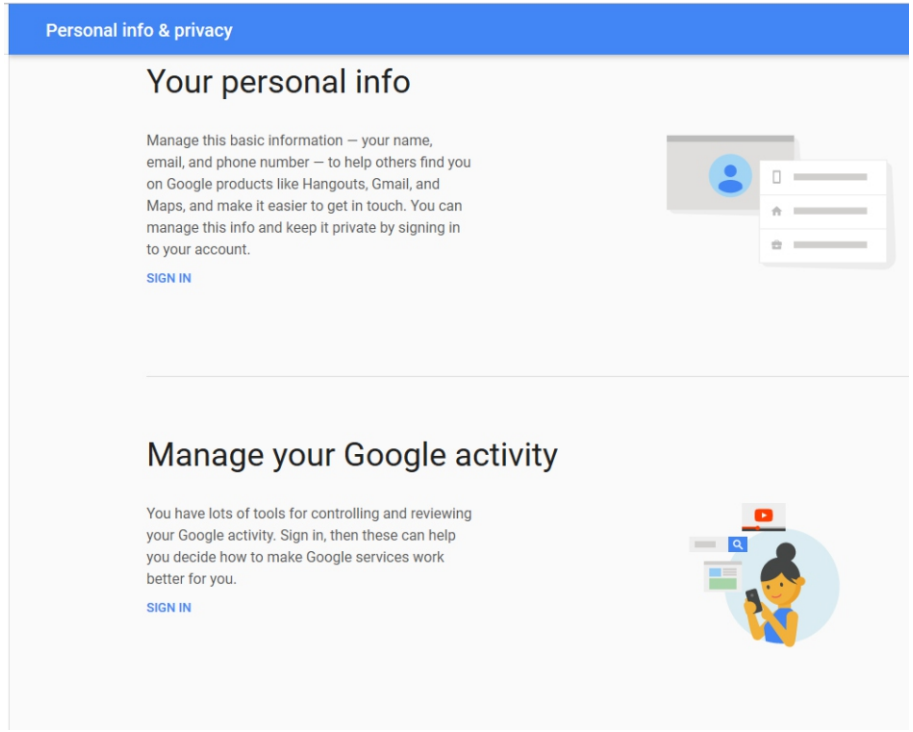


Simplify access to settings

Allow users to review their privacy settings in a clear, concise manner. Don't throw a bunch of UI controls at them.

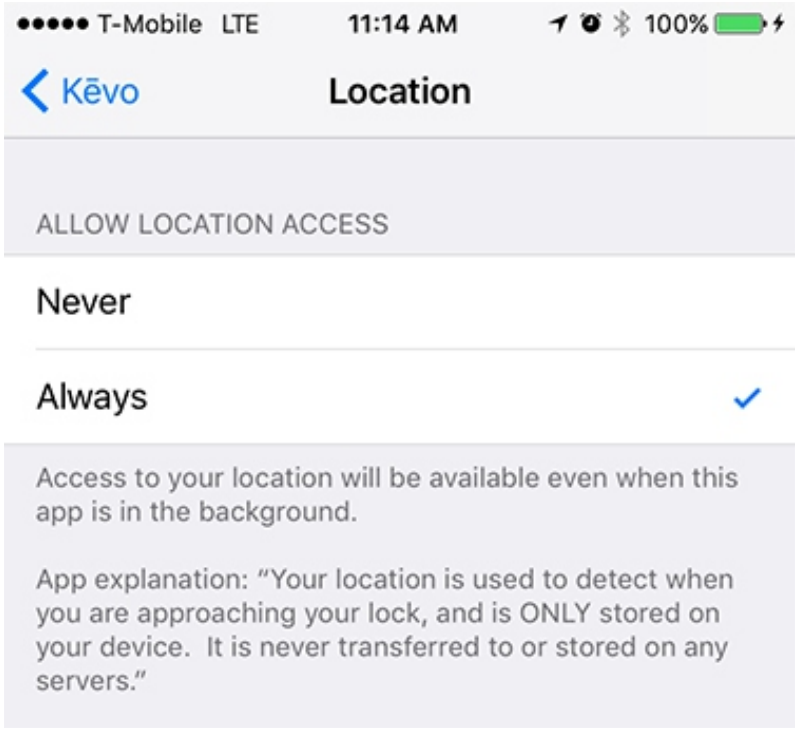
Position the settings in a way that matches the users mental model of how they think their data can be used.

Google's "My Account" Tool gives users access to their data across a wide range of Google features and user settings..



Be transparent about value

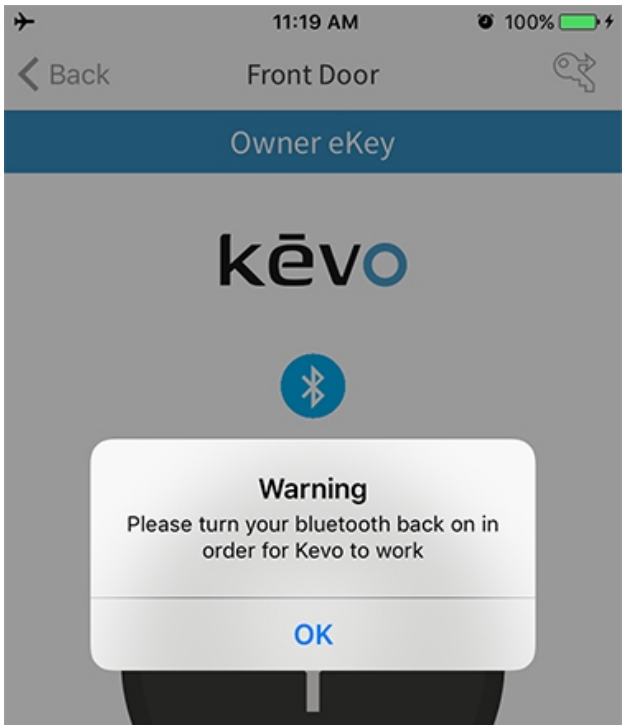
Be open and honest about internal benefits to using their information. If the collection doesn't have a real time benefit, but long term will improve the quality of service let them know.



Disclose privacy setting impacts on service

Disclose the impact a privacy decision may have on their user experience.

- Will a feature stop working?
- Will the whole application/service stop working?
- Can you provide a more basic, but functional experience to the user if they make a service change?



Online Trust Association trust framework

The Online Trust Association published their Internet of Things trust framework in March 2016. The latest version, 2.5 consists of 40 requirements and recommendations organizations can use for connected home and wearable products. Of those, a few key UX related recommendations include…

- Ensure privacy, security, and support policies are easily discoverable, clear and readily available for review prior to purchase, activation, download, or enrollment.
- Include strong authentication by default, including providing unique, system-generated or single use passwords; or alternatively use secure certificate credentials.
- Include strong authentication by default, including providing unique, system-generated or single use passwords; or alternatively use secure certificate credentials.
- Consider how to accommodate accessibility requirements for users who may be vision, hearing and or mobility impaired to maximize access for users of all physical capabilities.
- Develop communications processes to maximize user awareness of any potential security or privacy issues. Communications should be written maximizing comprehension for the general user's reading level.

- “IoT Trust Framework 2.5”, Online Trust Alliance

Thank You