# Privacy by Design

## Steps to help safeguard privacy

Heba Ramzy
Regional Director, Corporates Affairs
Microsoft Middle East and Africa

Accra Jan 28, 2016

# Key privacy concepts

| | |
|---|---|
| **Notice** | People are aware that you're collecting data from or about them, and know how you're going to use it. |
| **Choice** | People have controls over your use of the data you get from them. |
| **Access** | People can see what data you have from them, and ask you to change or remove it. |
| **Integrity** | You keep the data you get from people accurate and secure. |
| **Enforcement** | If a customer or authority brings up privacy problems, you can show you've done all the right things for privacy. |

# Basic privacy process:

1. Determine what data you need
2. Develop and document a system to manage and secure the data
3. Provide the right notice and consent
4. Write your Privacy Statement
5. Build the system, then collect and use data
6. Manage the data life cycle, grant customers access where necessary and appropriate and delete the data within a reasonable period

# Determine what data you need

1. **List the data you need:**
    - To provide the intended value to people
    - To maintain or improve that value
    - To meet your project needs and goals
2. **Look at each data point and remove any that aren't necessary**
3. **Write down how long you'll need to keep each type of data**
4. **Make a diagram (Data Flow Map) that shows:**
    - Where each piece of data will come from (public data or direct from customer)
    - How and where data will be transmitted and/or processed
    - How and where data will be stored

# Types of data to consider:

Uniquely identifiable info you collect from or about people
*Ex: Name and email address*

Information about identified people
*Ex: gender, voting history, approximate home location, friends list*

Metadata about what people do
*Ex: User spent 32 sec on level 6 of your app*

System information
*Ex: User is using a Dell Precision PC running Windows 7, browsing with Chrome*

Aggregated information
*Ex: residents of zip code 98052 have these commonalities*

# Develop a system to manage data

Now that you've figured out your data needs, plan how to manage it.

**Retention –**

- How long will you keep data?
- Will you enable on-demand and automated deletion?

**Security –** (next slide)

**Document these decisions -**

- What data, where, for how long, protected how, accessible by whom = **a data plan**

**Plan for communication –**

- How will you communicate this to your users in the privacy statement?
- How will the people on your project respond to inquiries about customer data or the data plan?

# Secure the data

Privacy is dependent on good security.

**For data transmissions, encrypt either your packets or your pipes**

- SSL: Secure Sockets Layer (or TLS: Transport Layer Security, the successor to SSL)

**For data storage – encrypt your storage at rest, plus**

- Only give people access to the data if they need access. For instance, access to the data should require authentication, and only the people who need access should be able to authenticate
- Computers that have access to the storage and processing should have well-maintained security, as well. Folks on your project may be trustworthy, but the viruses on their computers are not.

# Provide the right notice & consent

Plain language to describing your project is often the best privacy notice.
Here's more detailed guidance based on the type of data collection & use -

## Necessary data

The only data collected and used is to help provide the value of the app.

## Trackable data

You're collecting sensitive data, or you're sharing one person's data with other people.

## Extra data

You're collecting data unrelated to providing the value of the app, like, making money.

**Before they use your app, people should know**

**In the UI, provide**

- Clear language about what the app does

**In the privacy statement, share:**

- What data is collected or used
- Why that data is collected or used
- If a third party collects data through your app
- What you do to protect their data
- How to contact you about their data

**In the UI, provide**

- Everything in the first column
- A way they can say "Yes" explicitly (even if "no" means not using the app)

**In the privacy statement, share**

- Everything in the first column
- What to do if they change their mind
- That their info could be used to track them

**In the UI, provide**

- Everything in the first column
- A way they can say "Yes" explicitly (even if "no" means not using the app)

**In the privacy statement, share**

- Everything in the first column
- What to do if they change their mind
- What is the extra data you're collecting

# Write your Privacy Statement

**Tell people**

- What data you collect, and what you do with the data
- How you manage the data you collect or use
- If you're letting a third-party collect data
- If you're using their data to make money (monetization)
- How to communicate with you

**Your privacy statement should be available from the app and other locations where the customer can engage with your app or service.**
You can put a link to the privacy statement in the app footer, or in some other easy-to-find location.

*Hint: You've written this all down, already!*

Here's the difference:

The privacy statement is where you get to write down your practices so your customer will understand.

It's your opportunity to build your customer's trust, so they'll know you respect the value of the data you receive from them.

# Now you have…

A data plan that includes what data, data sources, storage, retention, security and access controls

A communication plan that supports customer inquiries

A user experience that provides clear insight into what happens with data

A privacy statement that communicates your privacy practices to the customer

…You're ready to build your project, and collect and use data!

# Collect and use data

Only collect and use data you've planned for

Don't surprise people: 'intuitive' and 'expected' are words that describe successful data usage

When things change:

- Update your data plan as necessary
- Determine whether and how to communicate those changes to your customer

# Key privacy concepts you've covered:

| | |
|---|---|
| **Notice** | Because of the UI and the Privacy Statement, people ARE aware that you have and are collecting data from them, and know how you're going to use it. |
| **Choice** | Because of the UI, people can consent to your use of the data you get from them. |
| **Access** | Because of the privacy statement, people can tell you to change or remove their data. |
| **Integrity** | By following your data management plan, you keep the data you get from people accurate and secure. |
| **Enforcement** | Using your data plan, data management plan, privacy policy, and UI, you can show you've done all the right things. |

# thank you!

hebar@microsoft.com

This document is for informational purposes only.