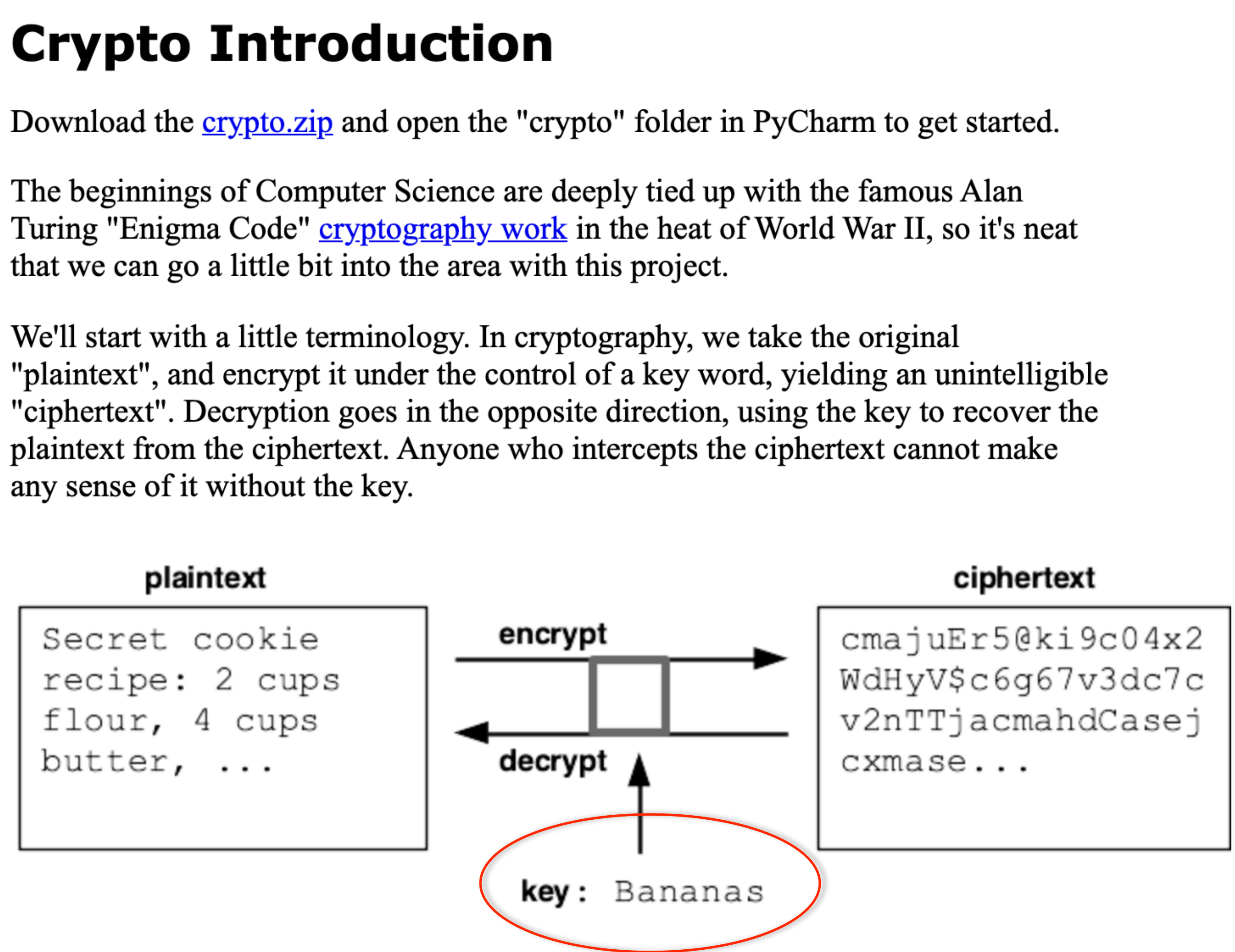
ENCRYPTION



Crypto Introduction

Download the crypto.zip and open the "crypto" folder in PyCharm to get started.

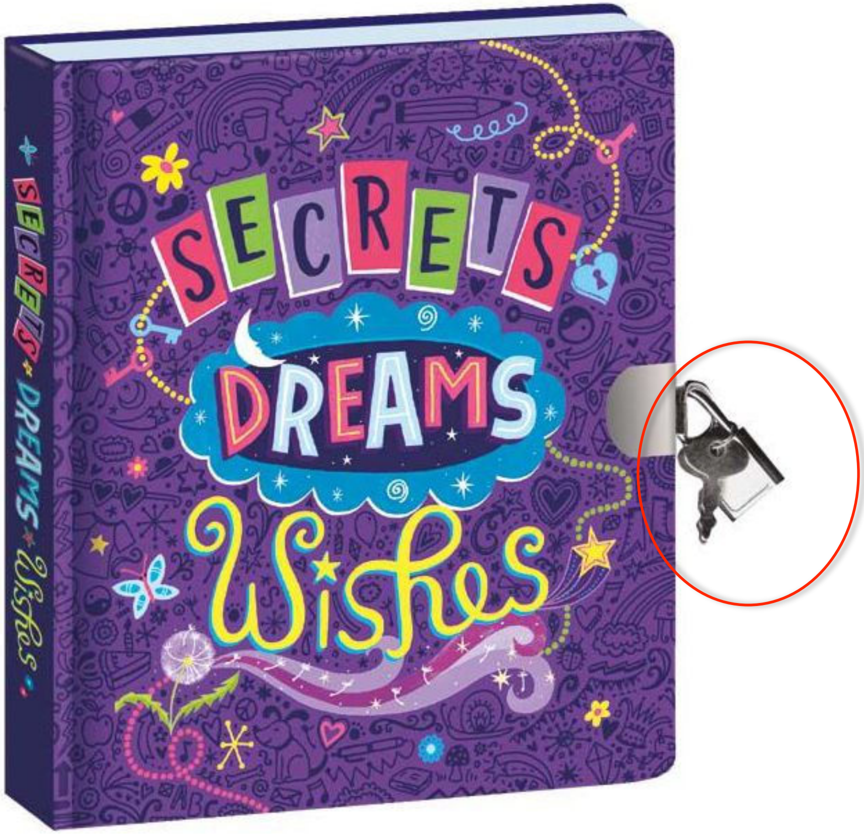
The beginnings of Computer Science are deeply tied up with the famous Alan Turing "Enigma Code" cryptography work in the heat of World War II, so it's neat that we can go a little bit into the area with this project.

We'll start with a little terminology. In cryptography, we take the original "plaintext", and encrypt it under the control of a key word, yielding an unintelligible "ciphertext". Decryption goes in the opposite direction, using the key to recover the plaintext from the ciphertext. Anyone who intercepts the ciphertext cannot make any sense of it without the key.

```
Secret cookie
recipe: 2 cups
flour, 4 cups
butter, ...
```

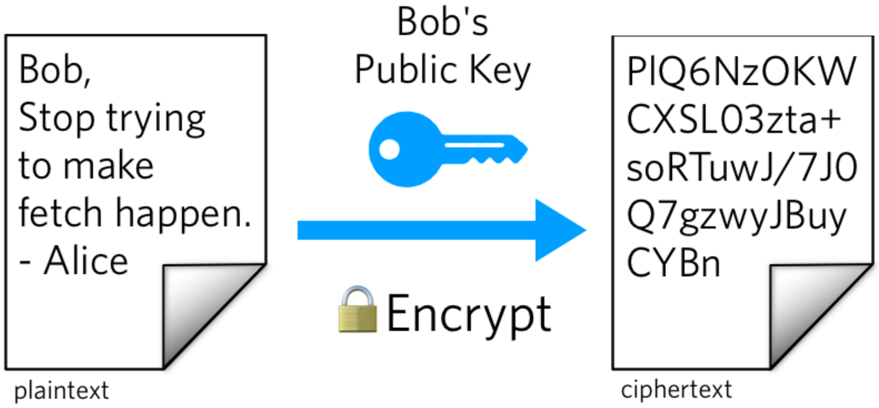
```
cmajuEr5@ki9c04x2
WdHyV$c6g67v3dc7c
v2nTTjacmahdCasej
cxmase...
```

SYMMETRIC KEY CRYPTOGRAPHY



PROBLEM: WHO HAS THE KEY?

ASYMMETRIC KEY CRYPTOGRAPHY:
WHEN ALICE MESSAGED BOB



Bob,
Stop trying
to make
fetch happen.
- Alice

plaintext

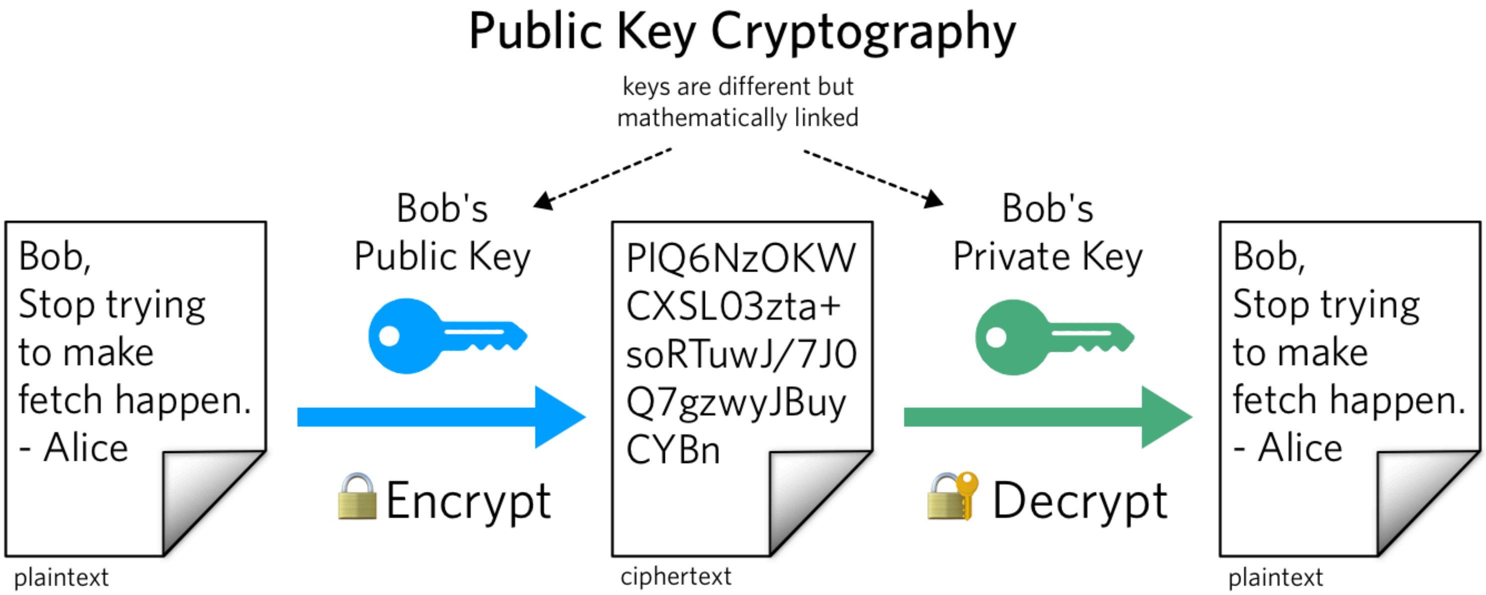
Bob's
Public Key

🔒Encrypt

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

ciphertext

ASYMMETRIC KEY CRYPTOGRAPHY:
WHEN ALICE MESSAGED BOB



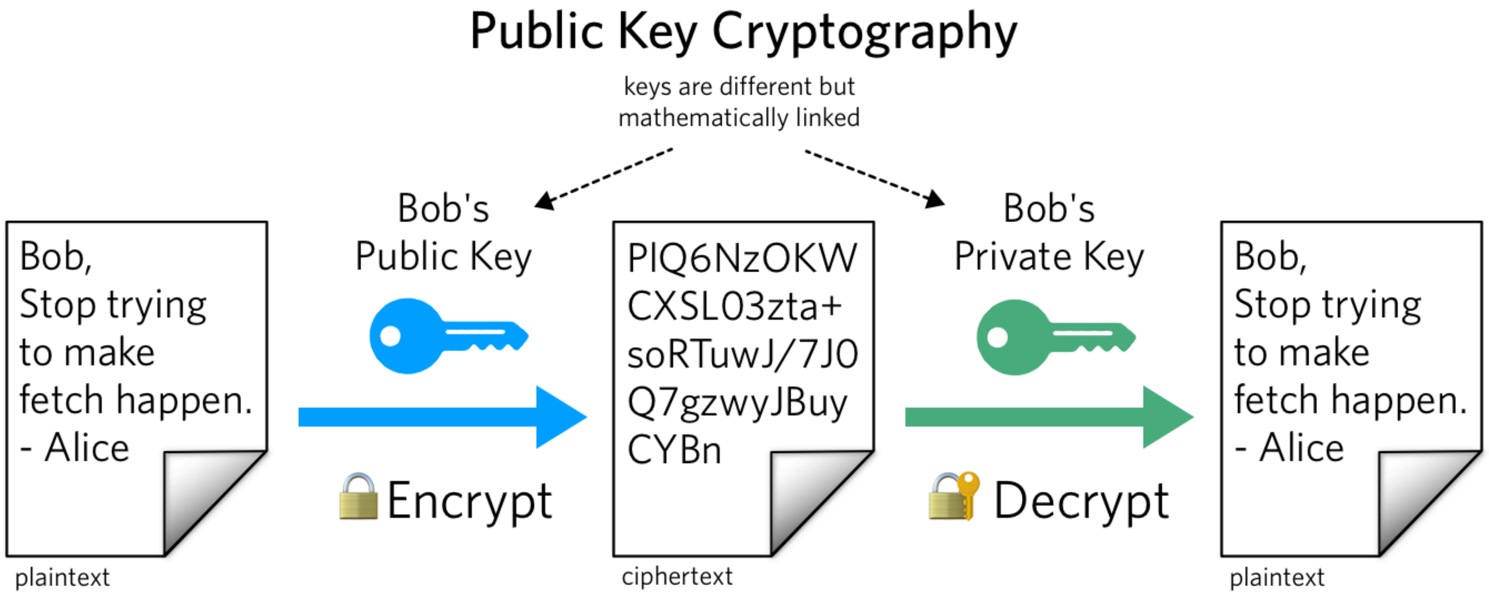
Bob,
Stop trying
to make
fetch happen.
- Alice

PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

Bob,
Stop trying
to make
fetch happen.
- Alice

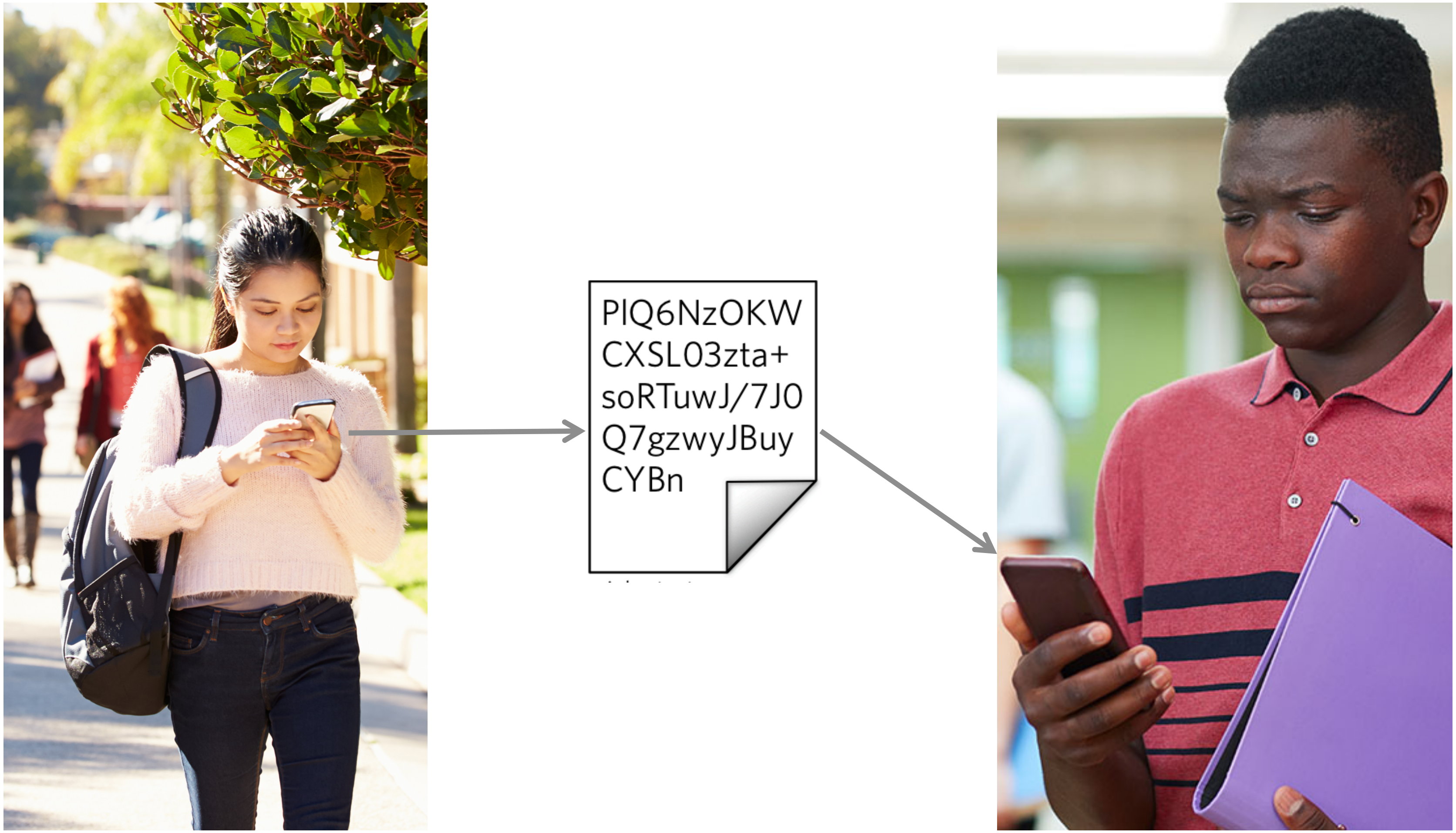
Only Bob can decrypt this message.

ASYMMETRIC KEY CRYPTOGRAPHY:
WHEN ALICE MESSAGED BOB


Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

Asymmetric key cryptography is often used in “end to end encryption”

END TO END ENCRYPTION



PIQ6NzOKW
CXSL03zta+
soRTuwJ/7J0
Q7gzwyJBuy
CYBn

END TO END ENCRYPTION FOR TEXTING

- **Signal** – one of the best
- **iMessage** – messages are end-to-end encrypted but not backups in iCloud
- **WhatsApp** – messages are end-to-end encrypted, but not backups (on Android) or metadata, like data about who is texting
- **Telegram** – can be end-to-end encrypted, but is not by default
- Others ...

WHY ENCRYPT YOUR DATA?

THE VALUE OF PRIVACY, BEYOND “I’VE GOT NOTHING TO HIDE”

HARMS OF PRIVACY VIOLATION TO THE INDIVIDUAL

- **Aggregation** — joining together small pieces of information that together reveal information a user might not want to share.
- **Distortion —** parties with access to data may draw incorrect conclusions from the data they have.
- **Inhibition —** surveillance can inhibit activity or speech, even without further threats, just because the user or citizen knows the activity will be observed or monitored**.**
- **Exclusion —** the citizen or user is excluded from seeing their own data and therefore does not know how it is being used and is not able to correct errors in the data.

Daniel Solove. “I’ve Got Nothing to Hide” and other Misunderstandings of Privacy (2007)

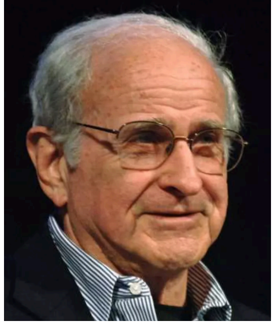
SOCIAL AND SOCIETAL HARMS OF PRIVACY VIOLATION

- **Preventing Intimacy —** Privacy enables social relationships (love, friendship), intimacy, and trust.
- **Breaking Trust —** Users or citizens may place less trust in governments (or companies) that collect and share their data – and reasonably so! Lack of trust in institutions has many downstream harms.

- **“Privacy should not be understood solely as an individual right…. Instead, privacy protects the individual because of the benefits it confers on society.” (Solove, 2008, 98, 171fn.).**

WHAT IS PRIVACY?

PRIVACY AS CONTROL OVER INFORMATION (WESTIN 1967)



Privacy as ...

the ability to determine for ourselves when, how, and to what extent information about us is communicated to others (Allan Westin, 1967)

This definitely of privacy works will with "the consent model" of privacy, where giving consent to share information means norms of privacy no longer apply. This is not the only model.

PRIVACY AS INACCESSIBILITY OF PERSONS (ALLEN 1988)

Privacy as ...

a degree of inaccessibility of persons, their mental states, and information about them to the senses and surveillance of others (Anita Allen 1988)

Types of privacy include:

- anonymity
- confidentiality
- seclusion
- solitude
- secrecy

PRIVACY AS CONTEXTUAL INTEGRITY: NISSENBAUM

1. Privacy is provided by appropriate flows of information.

2. Appropriate information flows are those that conform with contextual information norms

3. Contextual informational norms refer to five independent parameters:

- data subject
- sender
- recipient,
- information type
- transmission principle

4. Conceptions of privacy are based on ethical concerns that evolve over time

WHO IS RESPONSIBLE?

THE “MAN IN THE MIDDLE” IS RESPONSIBLE

THE "MAN IN THE MIDDLE" IS RESPONSIBLE

YOU ARE RESPONSIBLE : THE ETHICAL DUTY TO PROTECT YOUR OWN PRIVACY (ALLEN 2013)

Two kinds of ethical duties to protect your own privacy:

1. **"First order" duties to yourself to preserve your own privacy. Duties of self-respect and self-care to avoid harming yourself by violating your own privacy.**
2. **"Second order" duties to protect other people's privacy by protecting your own information.**
    1. E.g. if Alice and Bob are texting, Alice is responsible for protecting Bob's information by protecting their conversation.
    2. E.g. family members might be responsible for protecting each other by each protecting their own genetic information.

Dr. Anita L. Allen, An Ethical Duty to Protect One's Own Information Privacy, 64 Ala. Law Rev. 845 (2013).

HOW TO PROTECT YOUR OWN PRIVACY

- Use your new understanding of encryption to help yourself and others understand and change user settings
- Turn on end-to-end encryption in your messaging app or switch to a service that allows end-to-end encryption
- Follow the instructions on this guide to further secure your online life: https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy

THE DEVELOPER IS RESPONSIBLE

- Professional obligations of the designer or developer to protect the privacy of others
- We will discuss this more in the next ethics segment!