CS 111: Program Design I

Lecture 3: 5th Am., Python Basics

Robert H. Sloan & Richard Warner

University of Illinois at Chicago

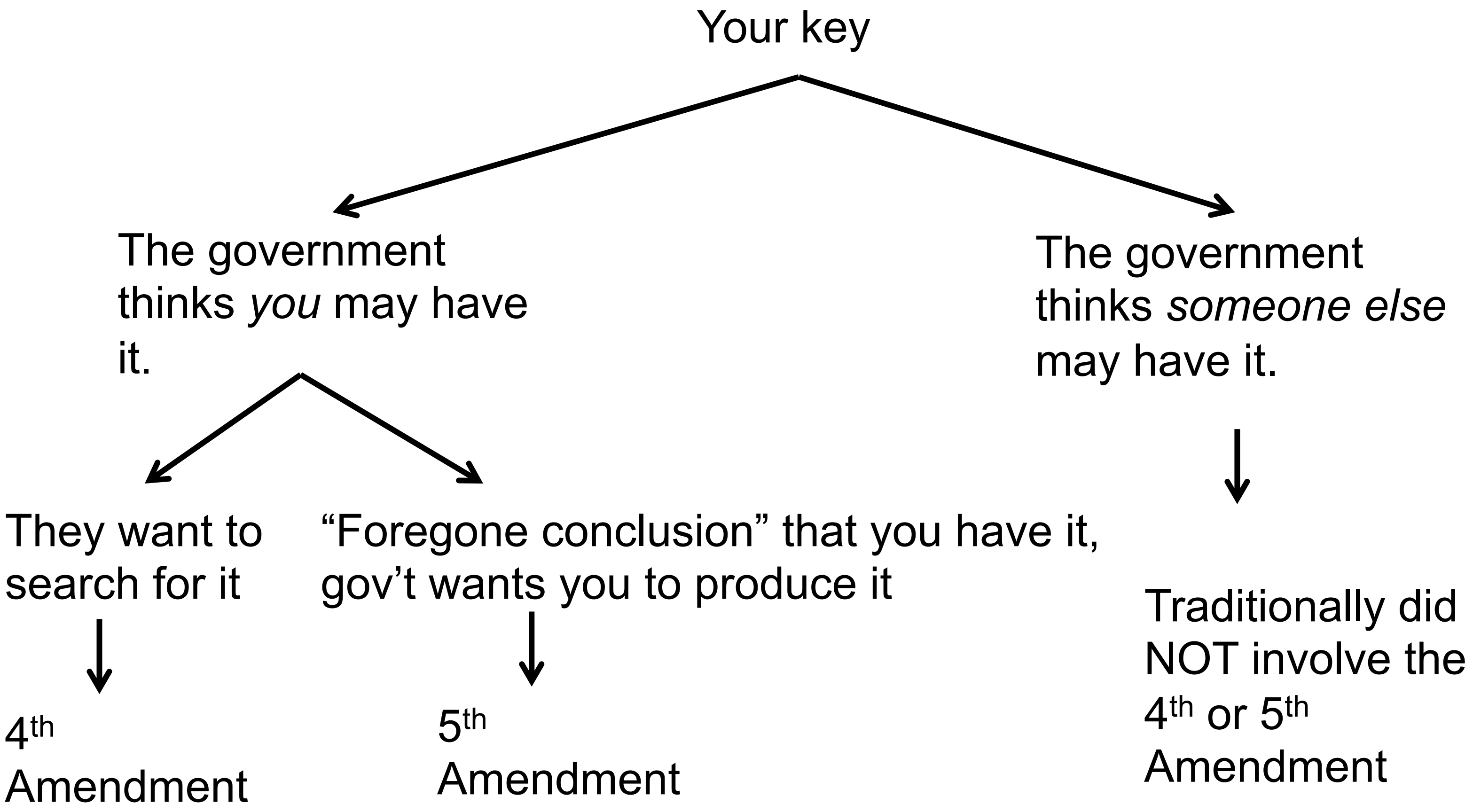
Tuesday, September 3, 2019

ENCRYPTION, PRIVACY, & GOVERNMENT POWER (CONT.)

Suspicion of Wrongdoing

- In *U. S. v. Doe*, Doe used a YouTube account the FBI suspected of exchanging child porn.
- The FBI determined that he accessed the Internet hotel rooms, so it tracked him to a hotel room, arrested him.
- It searched the room finding two laptops and five external hard drives.
- They could not decrypt the drives and so they subpoenaed the encryption key.
- Should Doe have to give up the key?
- A = Yes, B = No

Government Access Generally



Your key

The government thinks *you* may have it.

They want to search for it

4th Amendment

"Foregone conclusion" that you have it, gov't wants you to produce it

5th Amendment

The government thinks *someone else* may have it.

Traditionally did NOT involve the 4th or 5th Amendment

Did **you** register your clicker?

PYTHON BASICS

To build encryption and decryption need at least

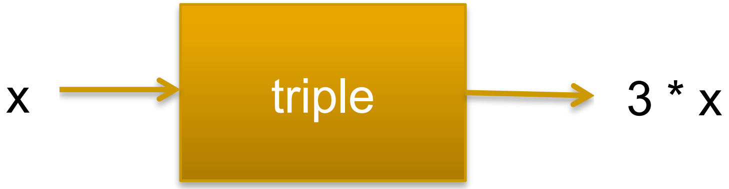
- **variables**
- **functions**
- **strings**
- Let’s start with very light look at functions that may help with Lab 2
- And move on to first light look at variables

Functions

- One of two ways (other is classes) to organize medium-small to huge computer programs
  - Zybooks ignores functions for first 1/3 of book and makes light use of them afterward
  - Zybooks heavily uses input(), which is almost never used except in a CS 1 course setting
- From Lab 2 to December, we'll use function *a lot* (and input() rarely outside Zybook activity)

Defining your own functions

```
def triple(x):
    return 3 * x
```



x

triple

3 * x

- Notice colon at end of def line
- Notice indentation
- Done using “tab” and absolutely necessary!

Functions can have more than one line

```
def triple(x):
    return 3 * x
```

```
def triple(x):
     my_answer = 3 * x
     return my_answer
```

Docstrings

```
def triple(x):
    """Input is number x, returns 3*x."""
    return 3 * x
```

- Teaching your program to talk to you
- Can access via help(triple)
- Convention: Enclose with 3 double quotes
    - Convention: Short, fit on one line
    - Make sure exactly 3 for both start and end!
- Use docstrings!

Comments

```python
# Tripling program
# Authors: Richard and Bob
# Date: September 52, 2019

def triple(x):
    """Input is number x, returns 3*x."""
    # Comments begin with a hash mark…
    return 3 * x
```

VARIABLES

Variables: Simple example

```
In [1]: justice1 = 'John Marshall'
In [2]: justice1
Out[2]: 'John Marshall'
In [3]: justice2 = 'Sandra Day O'Connor'
In [4]: justice2
Out[4]: "Sandra Day O'Connor"
In [5]: print(justice2)
Sandra Day O'Connor
```

print()

- Requires those parentheses!
- Prints out what you give it, and can give it sequence of things separated by commas
  - Optional end= to specify terminator; default newline (in book)

Code

```
print(3*5)
print('3*5')
```

At the end of this code, what will appear on the terminal?

```
3*5
3*5
```

A

```
15
15
```

B

```
15
3*5
```

C

```
3*5
15
```

D

E. I don’t know

Which of these Python 3 programs will print out an "A"?

```python
def printA():
    """I claim to print A"""
    print('A')
```

A

```python
def printA():
    """I claim to print A"""
    print 'A'
```

B

```python
def printA():
    """I claim to print A"""
    print('B')
```

C

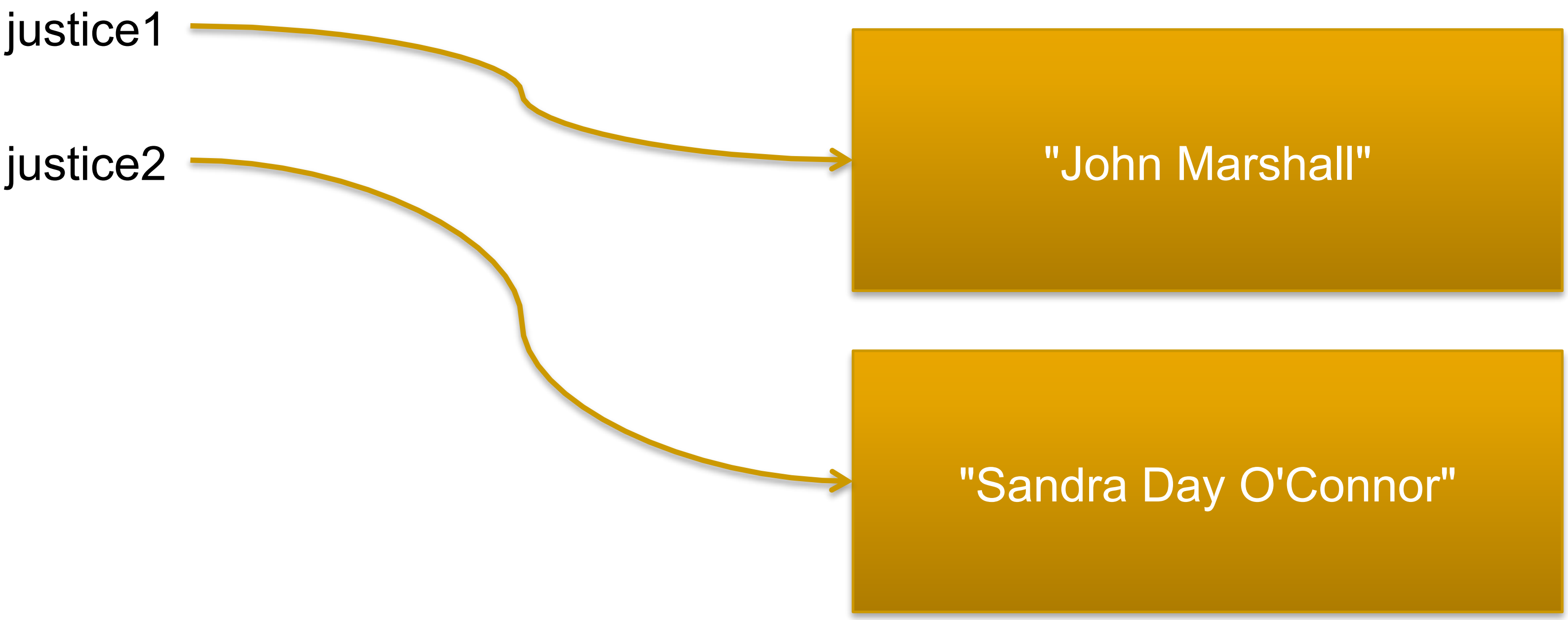
D. None of the above

Variables

- We want to tell computer to use specific value we put into its memory
  - (To print out a word, to add 2 numbers together, etc.)
- Much easier for us as humans to give these things names than to remember addresses

A box that holds a value

- Think of variable as box that holds a value (Pythonistas will say value or object more or less interchangeably), and variable's name as sticky note on the box



justice1

justice2

"John Marshall"

"Sandra Day O'Connor"

ENCRYPTION, PRIVACY, & GOVERNMENT POWER (CONT.)

Two Features

- The 5th Amendment debate revolves around a *rule*—the Fifth Amendment.
- The rule by itself provides no answer to the question.
- So why the obsession with the rule?

The Role of Rules

- We insist on decisions based on rules to ensure that we are governed by principles we all accept instead of someone's personal perspective.
- But *general* rules often do not determine their application to *particular* cases.
- To apply them we need to make *tradeoffs*.

The Fifth Amendment Tradeoff

- Adequate enforcement of laws requires adequate information about wrong doing.
- So: we need to balance the value of privacy against the needs of law enforcement.
- So: how much encryption of what kind should be legal when?
- That is the question underlying the encryption debate.

The Fifth Amendment

- 5th Amendment: “No person . . . shall be compelled in any criminal case to be a witness against himself . . .”
- You need to show three things:
  - (1) “I am being asked to testify.”
  - (2) “I am being compelled to do so.”
  - (3) “The testimony could incriminate me.”
- Is being required to decrypt encrypted data being compelled to testify?

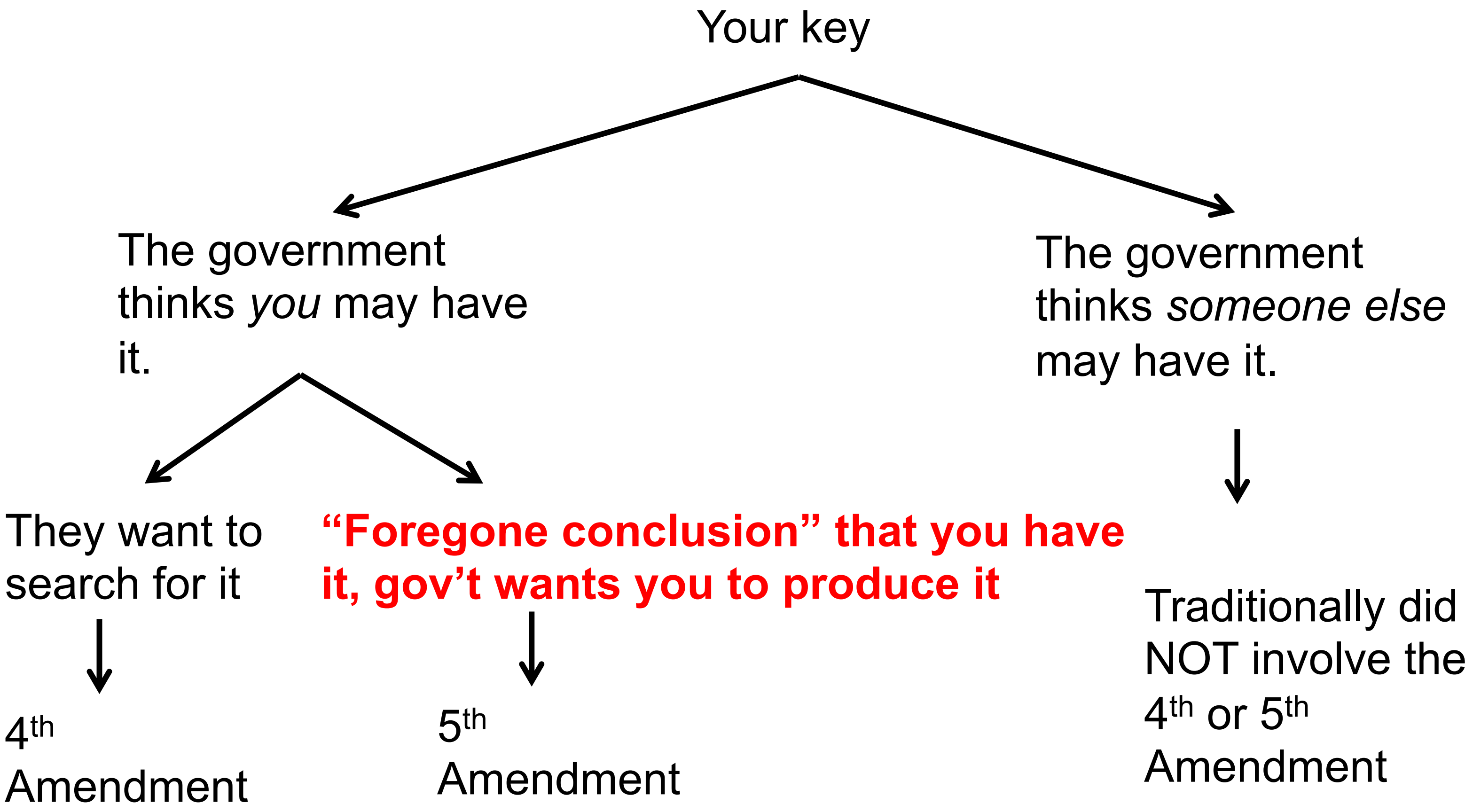
The First Test in *Doe*

- The Doe court held producing the key was testifying.
- Producing the key says,
  - “I know the files exist,”
  - “I can access them,’
  - “I can decrypt them.”
- Note: Other courts hold the opposite.

Testifying: *Two* Tests

- Producing the document is not testimony
  - if producing is a “mere physical act” where one does not “use one’s mind.”
    - Examples of *not* using: producing a key to a safe, putting on certain clothes.
  - if the contents of the document are a “foregone conclusion.”
    - Because the government does not learn anything it did not already generally know (it may not know the details).

Government Access Generally



Your key

The government thinks *you* may have it.

They want to search for it

4th Amendment

"Foregone conclusion" that you have it, gov't wants you to produce it

5th Amendment

The government thinks *someone else* may have it.

Traditionally did NOT involve the 4th or 5th Amendment

A Witness Against Himself

- Producing the key would tell the government something it does not know.
- On the court’s view, it is not a foregone conclusion that there is child pornography on the drives.
- Because the encrypted drives could be empty.
  - Is that a good reason?
  - *Any* encrypted drive could be empty.
  - So a high hurdle.