VIPERLIB

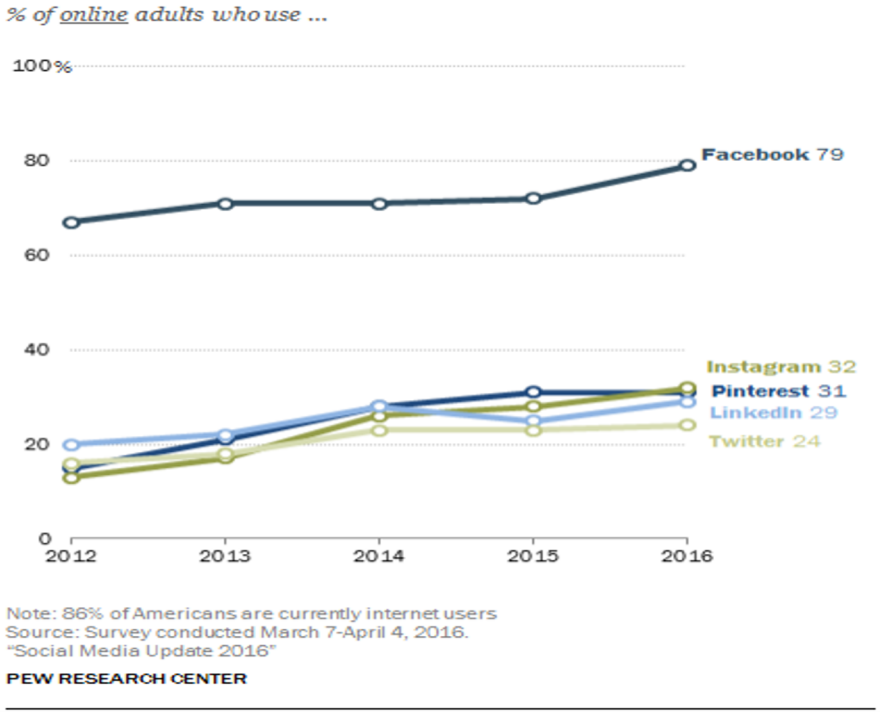
SUPERVISED BY: JASMINE DEHART

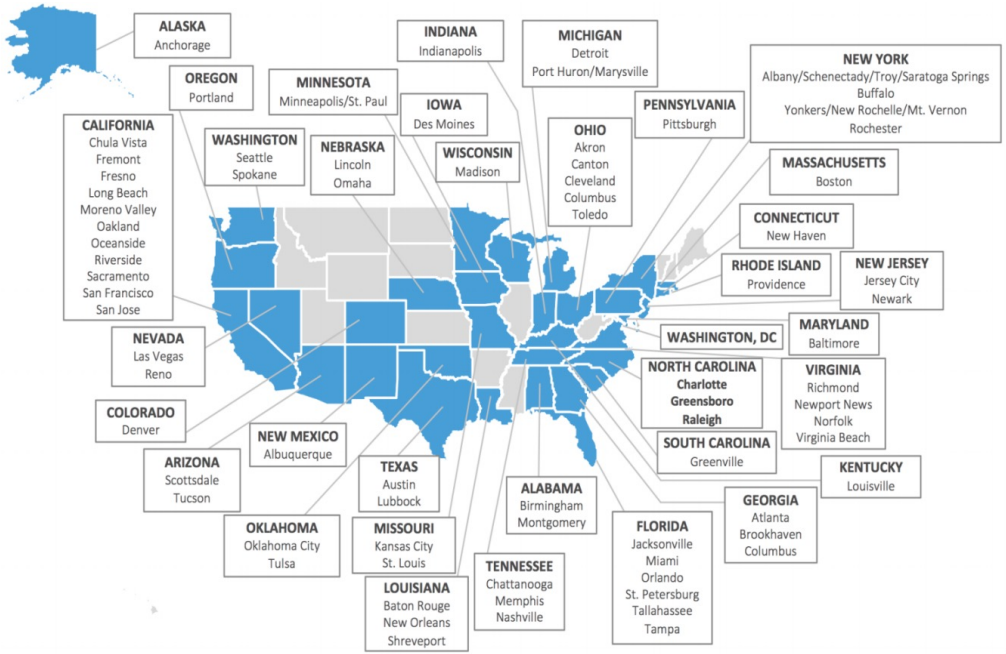
LAB ADVISOR: CHRISTAN GRANT

OU DATA LAB

An open-source Python Library for mitigating privacy with Machine Learning

Overview





Greenwood, S., Perrin, A., & Duggan, M. (2016). Social media update 2016. Pew Research Center, 11, 83.

Examples

Greenwood, S., Perrin, A., & Duggan, M. (2016). Social media update 2016. Pew Research Center, 11, 83.

Visual Privacy Leak Example
Hawaii Emergency Agency
source: Twitter


John Smith
123 Broadway
City, State 12345

John Smith, 123 Broadway , City, State 12345

Director
Corporation
123 Pleasant Lane
City, State 12345

Location

Dangers:

- Burglary
- Stalking
- Kidnapping

Dangers:

- Identity theft
- Financial threat
- Burglary

Identity

Asset

Dangers:

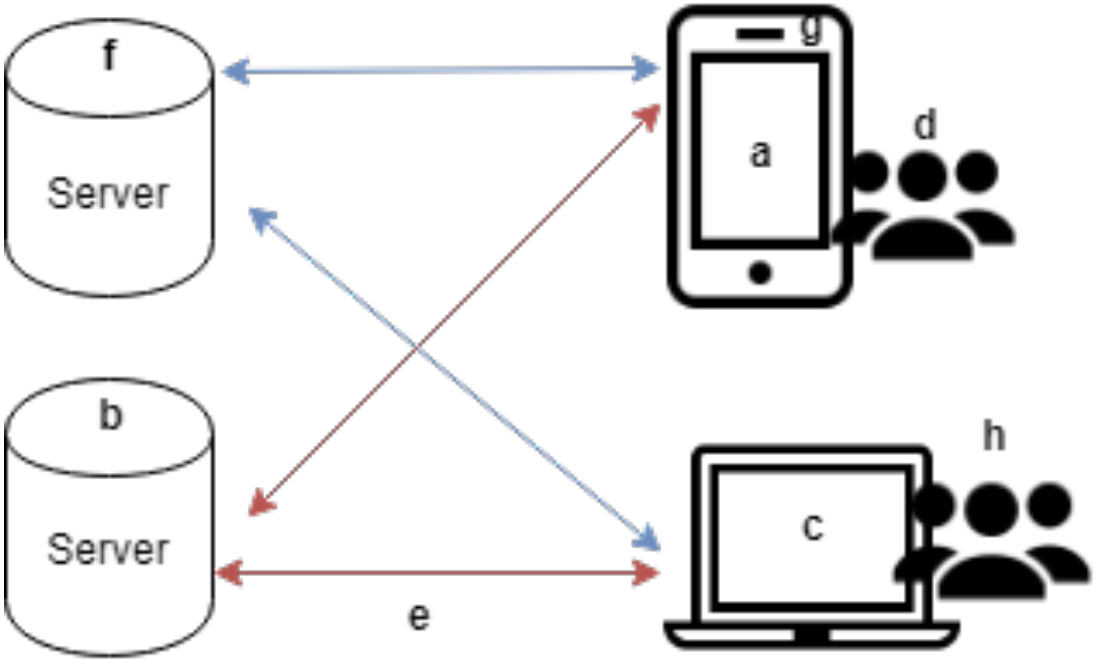
- Financial threat
- Burglary
- Digital kidnapping
- Explicit websites

WHAT IS VIPER?

VIPER is the Visual Inspection of Personally Exposed Records

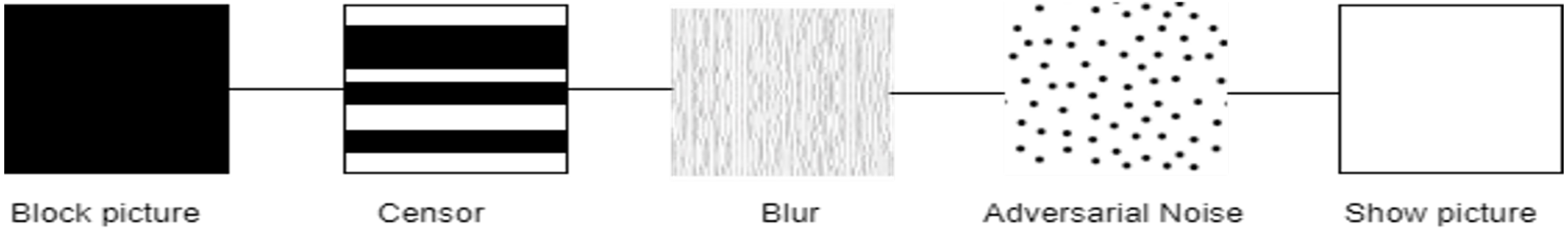
- Understand perspectives of private content
- Propose mitigation techniques and libraries
- Research privacy in the domains of social media, smart cities, and connected networks

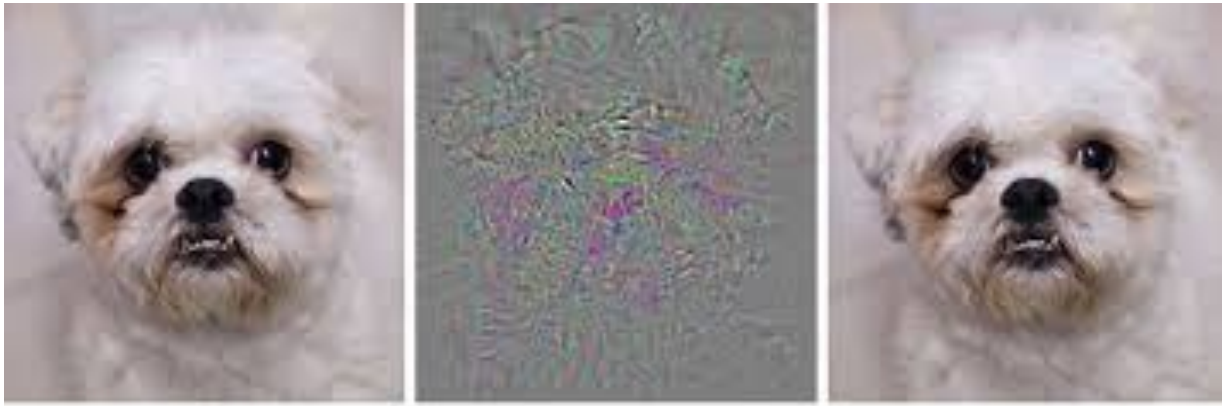
Mitigation Techniques



a - *Client app*
b - *Privacy Patrol*
c - *Chaperone bot*
d - *Category tagger*
e - *Privacy Scorer*
f - *Server app*
g - *Interceptor*
h - *Redactor*

Redaction Spectrum





Adversarial Noise Example

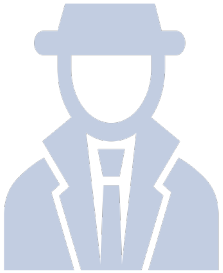
VIPERLib Project

CREATE OBJECT DETECTION MODEL

IMPLEMENT REDACTION TECHNIQUES

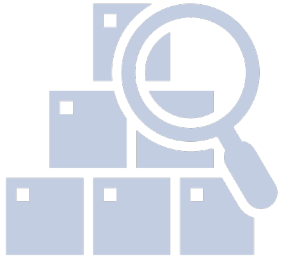
ESTABLISH VIPERLIB

Additional Tasks

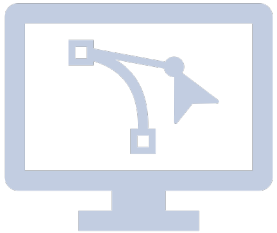


Estimate likelihood an image can be uncovered after redaction

How much the object is showing after redaction



Detect or count # of objects in an image



Application design for mitigation techniques

Questions?

OU Data Lab → *https://oudatalab.com/*
Jasmine DeHart → *https://jasminedehart.com/*
Christan Grant → *http://www.christangrant.com/*