TOWARDS TRUSTWORTHY ML: RETHINKING SECURITY AND PRIVACY FOR ML. INTERNATIONAL CONFERENCE ON LEARNING REPRESENTATIONS. 26 SEPTEMBER 2020.

CONTEXT, RESEARCH, REFUSAL

PERSPECTIVES ON ABSTRACT PROBLEM-SOLVING

DR SEETA PEÑA GANGADHARAN

Outline

PART 1 Context, Context Sensitization

PART 2 Refusal: Rectification, Obfuscation, Abolition

PART 3 The Problem with Abstraction

Part 1

Context, Context Sensitization

TOWARDS TRUSTWORTHY ML: RETHINKING SECURITY AND PRIVACY FOR ML. INTERNATIONAL CONFERENCE ON LEARNING REPRESENTATIONS. 26 SEPTEMBER 2020.

https://drive.google.com/file/d/1TTxz494t6Wfs1mvAAHbgNKTn_VQY1ZQo/view?ts=5e8b8d0f

Clifford Christians

James Carey

[I]n studying humans we are examining a creative process whereby people produce and forms of life and society and systems of meaning and value (1989, p. 346).

The Moral Character of Cryptographic Work*

Phillip Rogaway

Department of Computer Science
University of California, Davis, USA
rogaway@cs.ucdavis.edu

December 2015
(minor revisions March 2016)

Abstract. Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension. The Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe that it does. I call for a community-wide effort to develop more effective means to resist mass surveillance. I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work.

Keywords: cryptography · ethics · mass surveillance · privacy · Snowden · social responsibility

Preamble. Most academic cryptographers seem to think that our field is a fun, deep, and politically neutral game—a set of puzzles involving communicating parties and notional adversaries. This vision of who we are animates a field whose work is intellectually impressive and rapidly produced, but also quite inbred and divorced from real-world concerns. Is this what cryptography *should* be like? Is it how we *should* expend the bulk of our intellectual capital?

For me, these questions came to a head with the Snowden disclosures of 2013. If cryptography's most basic aim is to enable secure communications, how could it *not* be a colossal failure of our field when ordinary people lack even a modicum of communication privacy when interacting electronically? Yet I soon realized that most cryptographers didn't see it this way. Most seemed to feel that the disclosures didn't even implicate us cryptographers.

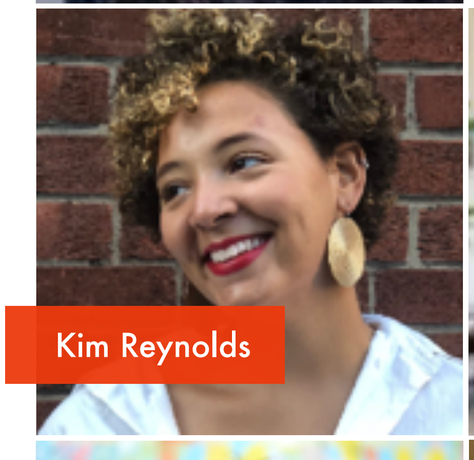
I think that they do. So I want to talk about the moral obligations of cryptographers, and my community as a whole. This is not a topic cryptographers routinely discuss. In this post-Snowden era, I think it needs to be.

Part 2

Refusal: Rectification, Obfuscation, Abolition

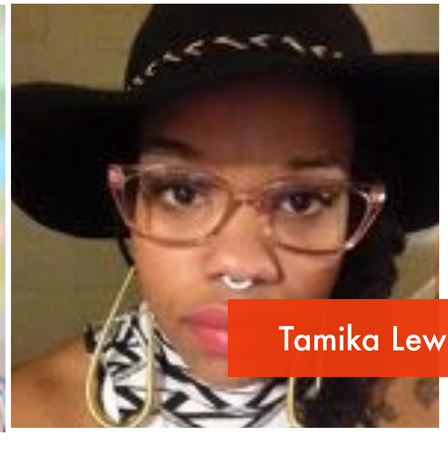
TOWARDS TRUSTWORTHY ML: RETHINKING SECURITY AND PRIVACY FOR ML. INTERNATIONAL CONFERENCE ON LEARNING REPRESENTATIONS. 26 SEPTEMBER 2020.


Mariella Saba


Kim Reynolds


Seeta Peña Gangadharan


Tawana Petty


Tamika Lewis

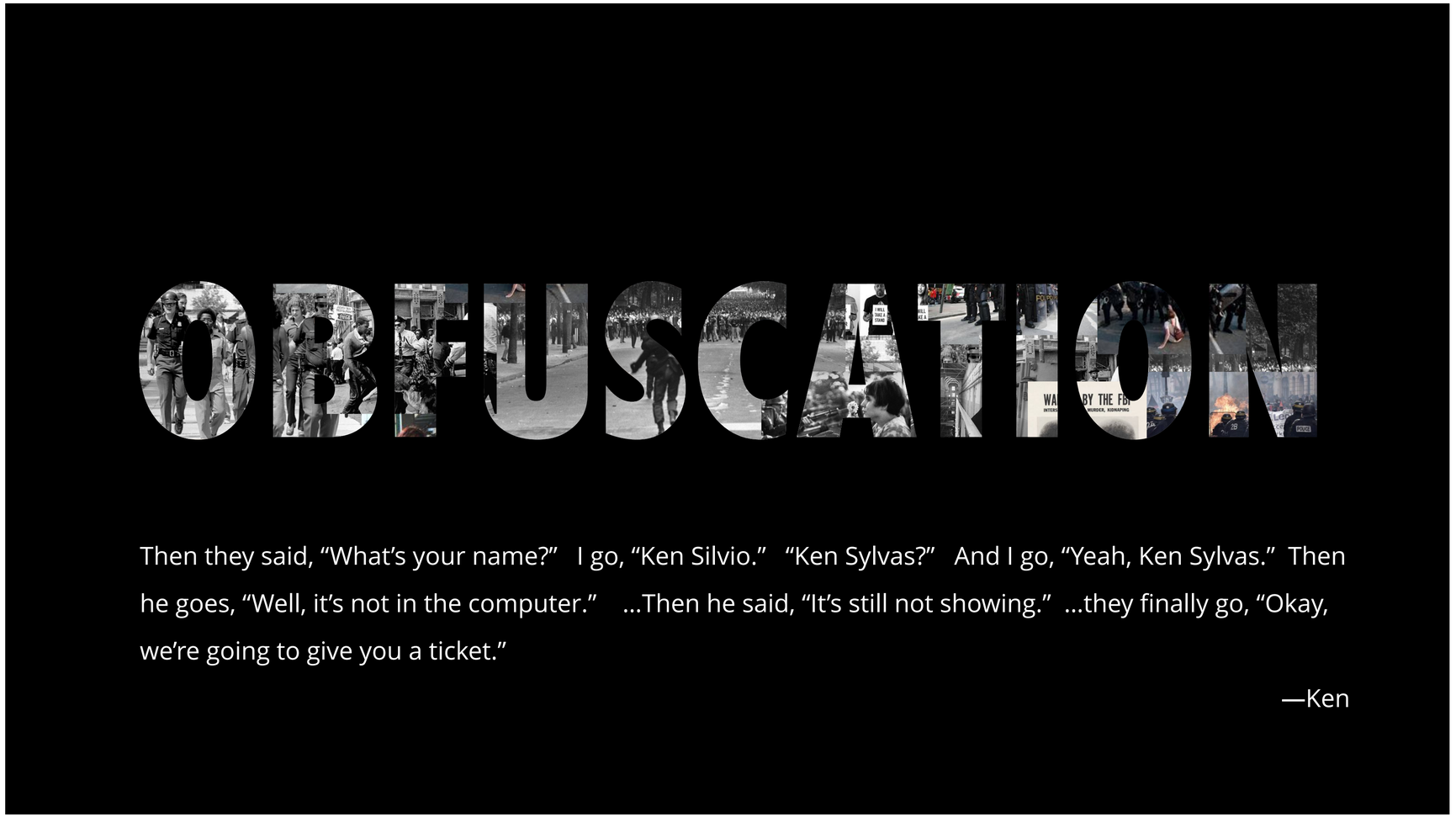
Our Data Bodies

- Impact of data-driven systems and data collection on marginalized communities
- Community-centered, participatory research in Charlotte, Detroit, & Los Angeles
- 140 interviews + reflective focus groups + participatory workshops


REFUSAL
I WILL
TAKE A
STAND
CAUTION
ANGELA

"The grievances were not in the file and I had seven, at least. Good thing I made copies of my own, I took pictures of it. Any time before I turned it in, I took pictures of it so … I have so much footage that I have to go through…But everything should be in your file grievances and all."

—Mellow



Then they said, “What’s your name?” I go, “Ken Silvio.” “Ken Sylvas?” And I go, “Yeah, Ken Sylvas.” Then he goes, “Well, it’s not in the computer.” …Then he said, “It’s still not showing.” …they finally go, “Okay, we’re going to give you a ticket.”

—Ken


ABOLITION
At this juncture in Detroit's history, there are two clear paths forward. The first path sees more surveillance...The second path is different... It guards privacy while increasing trust in the government. It both protects and serves.
— Detroit Community Technology Project

Part 3

The Problem of Abstraction

ABSTRACTION

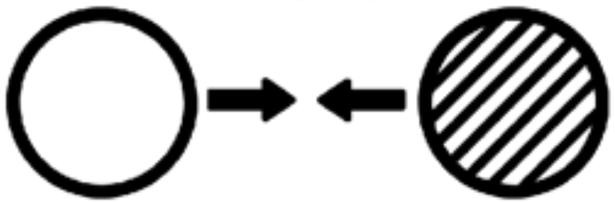
Privacy

Health

Collective well-being

Tech welfare

FRICTION



ALIGNMENT

Thank you.

DR SEETA PEÑA GANGADHARAN

Dr. Seeta Peña Gangadharan