Policy Impact with Computer Science

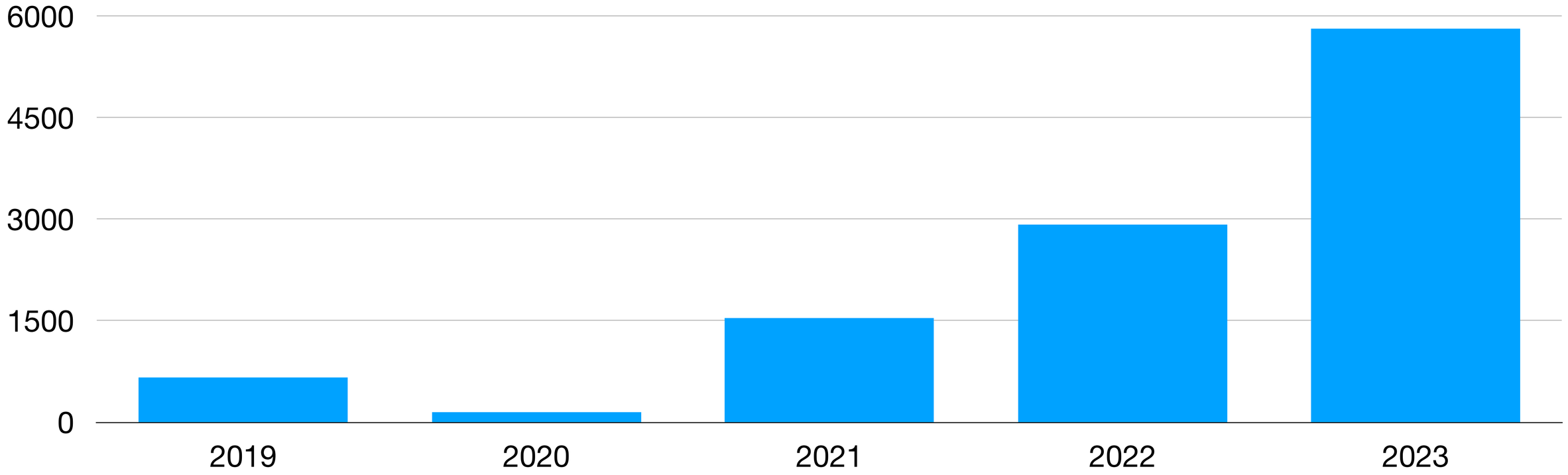
Why It's Needed,
How to Achieve It, and
Why We Don't

Jonathan Mayer
Princeton University
July 14, 2025

This is a machine gun.

26 U.S.C. § 5845(b)*

Machine Gun Conversion Devices Recovered by U.S. Law Enforcement



ATF Firearms Trace Data


DO NOT ENTER
SLOW
Proceed over Inspection Ramp
Speed Limit 1-3 MPH
NO DELIVERIES
All Deliveries Use Rear Entrance
SPEED LIMIT 10
STOP
244 Needy Road
ALL PERSONS ENTERING THESE PREMISES MUST PRESENT PROPER I.D. TO OFFICER ON DUTY
NO VA CENTER ENTRANCE
No access to the VA Medical Center

OMB No. 1140-0020

U.S. Department of Justice
Bureau of Alcohol, Tobacco, Firearms and Explosives

Firearms Transaction Record

WARNING: The information you provide will be used to determine whether you are prohibited by Federal or State Law from receiving a firearm, or whether Federal or State Law prohibits the sale or disposition of a firearm to you. Certain violations of the Gun Control Act, 18 U.S.C. § 921 et. seq., are punishable by up to 15 years imprisonment and/or up to a $250,000 fine. Any person who exports a firearm without a proper authorization from either the Department of Commerce or the Department of State, as applicable, is subject to a fine of not more than $1,000,000 and up to 20 years imprisonment.

Read the Notices, Instructions, and Definitions on this form. Prepare in original only at the licensed premises (including business temporarily conducted from a qualifying gun show or event in the same State in which the premises is located) unless the transaction qualifies under 18 U.S.C. § 922(c). **All entries must be handwritten in ink unless completed under ATF Rul. 2016-2.** PLEASE PRINT.

Transferor's/Seller's Transaction Number (if any)

Section A - Must Be Completed By Transferor/Seller Before Transferee/Buyer Completes Section B

1. Manufacturer and Importer (if any), or Privately Made Firearm (PMF) (If the Manufacturer and Importer are different, include both.)	2. Model (if designated)	3. Serial Number	4. Type	5. Caliber or Gauge
1.				
2.				
3.				

6. Total Number of Firearms to be Transferred (Please spell total number e.g., one, two, etc. Do not use numerals.)

7. Check if any part of this transaction is a pawn redemption. ☐
Record Line Number(s) From Question 1:

8. Check if any part of this transaction is to facilitate a private party transfer. ☐

Section B - Must Be Completed Personally By Transferee/Buyer

9. Transferee's/Buyer's Full Name (If legal name contains an initial only, record the initial followed by "IO" in quotes. If no middle initial or name, record "NMN".)

Last Name (including suffix, e.g., Jr, Sr, II, III) | First Name | Middle Name

10. Current State of Residence and Address (U.S. postal abbreviations are acceptable. Cannot be a post office box.)

Number and Street Address | City | Reside in City Limits? ☐ Yes ☐ No ☐ Unknown | State | ZIP Code | County/Parish/Borough

11. Place of Birth
U.S. City **and** State **-OR-** Foreign Country

12. Height
Ft. _____
In. _____

13. Weight (lbs.)

14. Sex
☐ Male
☐ Female
☐ Non-Binary

15. Birth Date
Month | Day | Year

16. Social Security Number (optional, but will help prevent misidentification)

17. Unique Personal Identification Number (UPIN) or Appeals Management Database Identification (AMD ID) (if applicable)

18.a. Ethnicity
☐ Hispanic or Latino
☐ Not Hispanic or Latino

18.b. Race (Select one or more race in 18.b. Both 18.a. and 18.b. must be answered.)
☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Native Hawaiian or Other Pacific Islander
☐ White

19. Country of Citizenship: (Check/List more than one, if applicable. Nationals of the United States may check U.S.A.)
☐ United States of America (U.S.A.) ☐ Other Country/Countries (Specify):

20. If you are an alien, record your U.S.-issued alien or admission number (AR#, USCIS#, or I94#):

21. Answer the following questions by checking or marking either the "yes" or "no" box to the right of the questions:	Yes	No
a. Are you the actual transferee/buyer of all of the firearm(s) listed on this form and any continuation sheet(s) (ATF Form 5300.9A)? **Warning: You are not the actual transferee/buyer if you are acquiring any of the firearm(s) on behalf of another person. If you are not the actual transferee/buyer, the licensee cannot transfer any of the firearm(s) to you.** Exception: If you are only picking up a repaired firearm(s) for another person, you are not required to answer 21.a. and may proceed to question 21.b.	☐	☐
b. Do you intend to sell or otherwise dispose of any firearm listed on this form and any continuation sheet(s) in furtherance of any felony or other offense punishable by imprisonment for a term of more than one year, a Federal crime of terrorism, or a drug trafficking offense?	☐	☐
c. Are you under indictment or information in any court for a **felony,** or any other crime for which the judge could imprison you for more than one year, or are you a current member of the military who has been charged with violation(s) of the Uniform Code of Military Justice and whose charge(s) have been referred to a general court-martial?	☐	☐
d. Have you ever been convicted in any court, including a military court, of a **felony,** or any other crime for which the judge could have imprisoned you for more than one year, even if you received a shorter sentence including probation?	☐	☐
e. Are you a fugitive from justice?	☐	☐

DEPARTME OF THE

BUREAU OF ALCOHOL TOBACCO

FIREARMS TRANSACTION RECORD PA

are in original only. All entries on this form must be in ink

SECTION A - MUST BE COMP

REE'S (Buyer) NAME (Last, First, Middle)

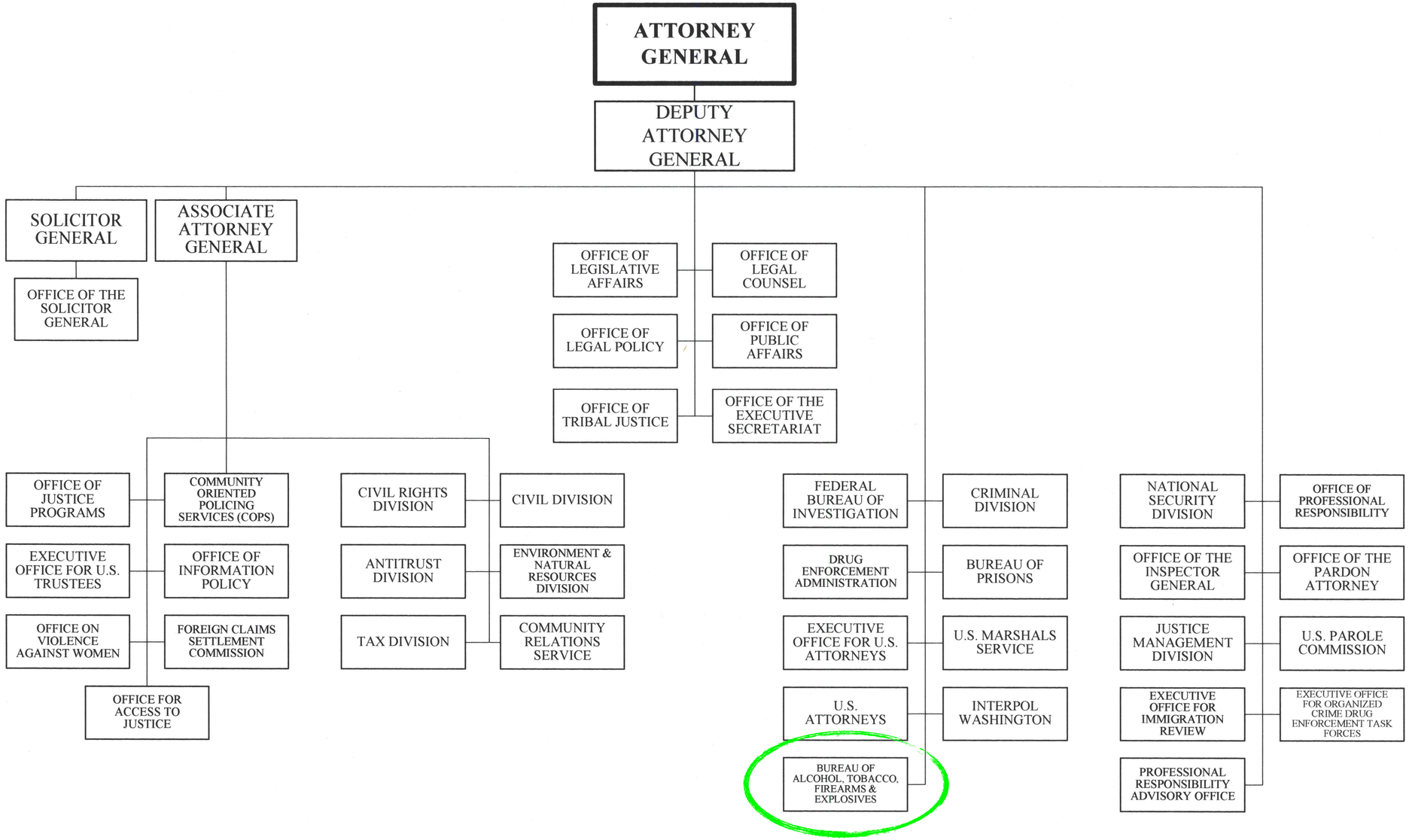
ROBERT


F MISSION
FIREARMS TRACING
FIREARMS TRACING
Trace

7-10 days

For a routine crime gun trace, on average

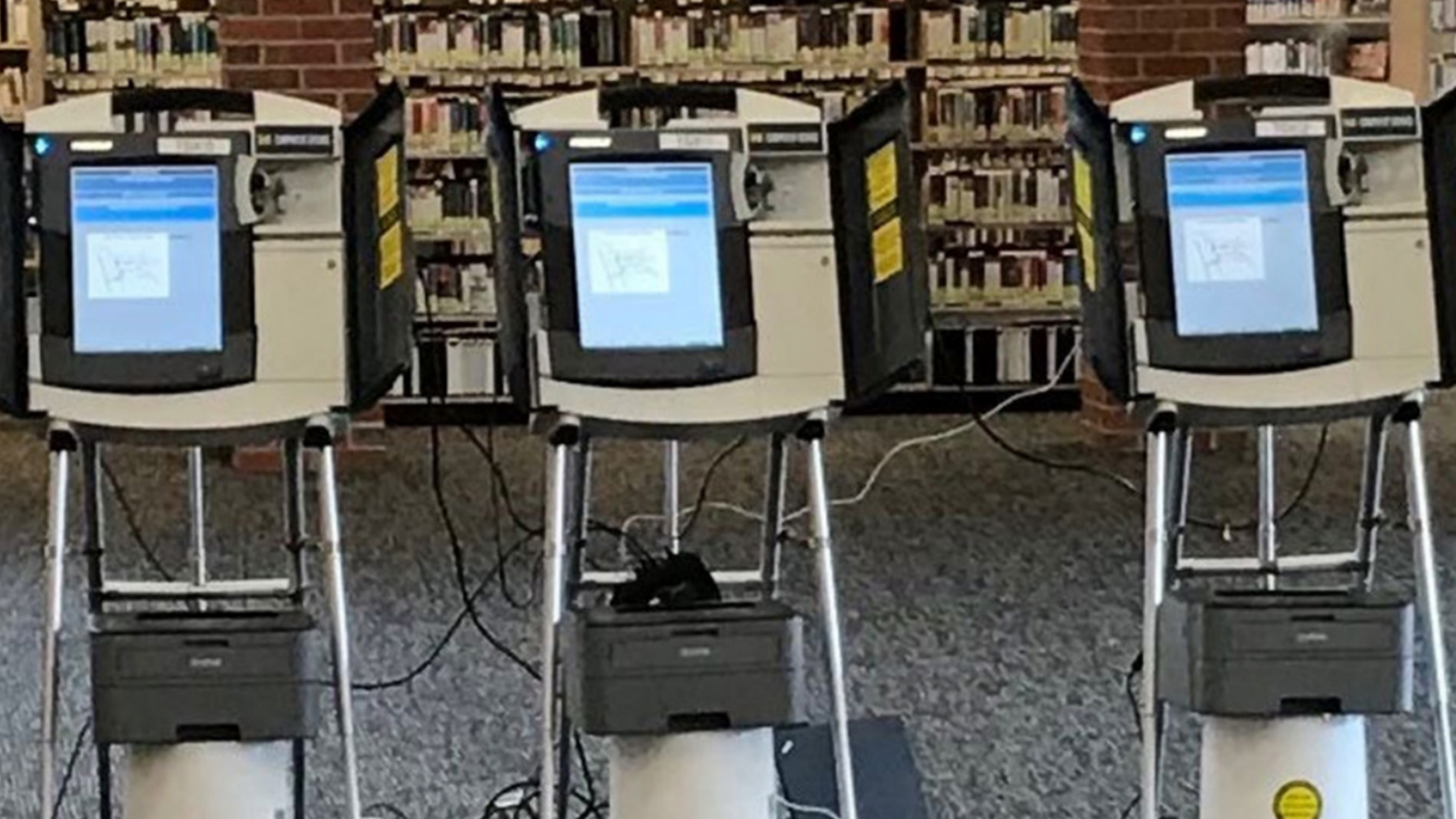
U.S. DEPARTMENT OF JUSTICE



Approved by: _____ Date: 8/17/23

MERRICK B. GARLAND
Attorney General

Computer science can save lives.



Computer science can protect democracy.

DAMIAN WILLIAMS
United States Attorney for the
Southern District of New York
Attorney for the United States of America
By: ELLEN BLAIN
DAVID J. KENNEDY
JACOB LILLYWHITE
CHRISTINE S. POSCABLO
Assistant United States Attorneys
86 Chambers Street, Third Floor
New York, New York 10007
Telephone (212) 637-2733
Facsimile (212) 637-0033
david.kennedy2@usdoj.gov

KRISTEN CLARKE
Assistant Attorney General
SAMEENA SHINA MAJEED
Chief, Housing and Civil Enforcement Section
R. TAMAR HAGLER
Deputy Chief
JUNIS L. BALDON
HARIN C. SONG
KINARA A. FLAGG
Trial Attorneys
Civil Rights Division
U.S. Department of Justice
950 Pennsylvania Avenue NW – 4CON
Washington, DC 20530
Tel.: (202) 353-1339
Fax: (202) 514-1116

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

META PLATFORMS, INC., f/k/a FACEBOOK, INC.,

Defendant.

COMPLAINT

22 Civ. _____ (____)

Jury Trial Demanded

Computer science can protect civil rights.

Computer science can save lives
protect democracy
protect civil rights
enable accountability
improve programs
protect data
. . .
make policy better

Computer science can create new capabilities
provide enforcement leads
change the solution space
highlight problems
provide facts & arguments
evaluate efficacy
call out BS
forecast developments
offer credibility
overcome partisanship
…

Plus, public policy can surface important technical problems for computer science.

The importance of technology in public policy and law is skyrocketing.

~5-10

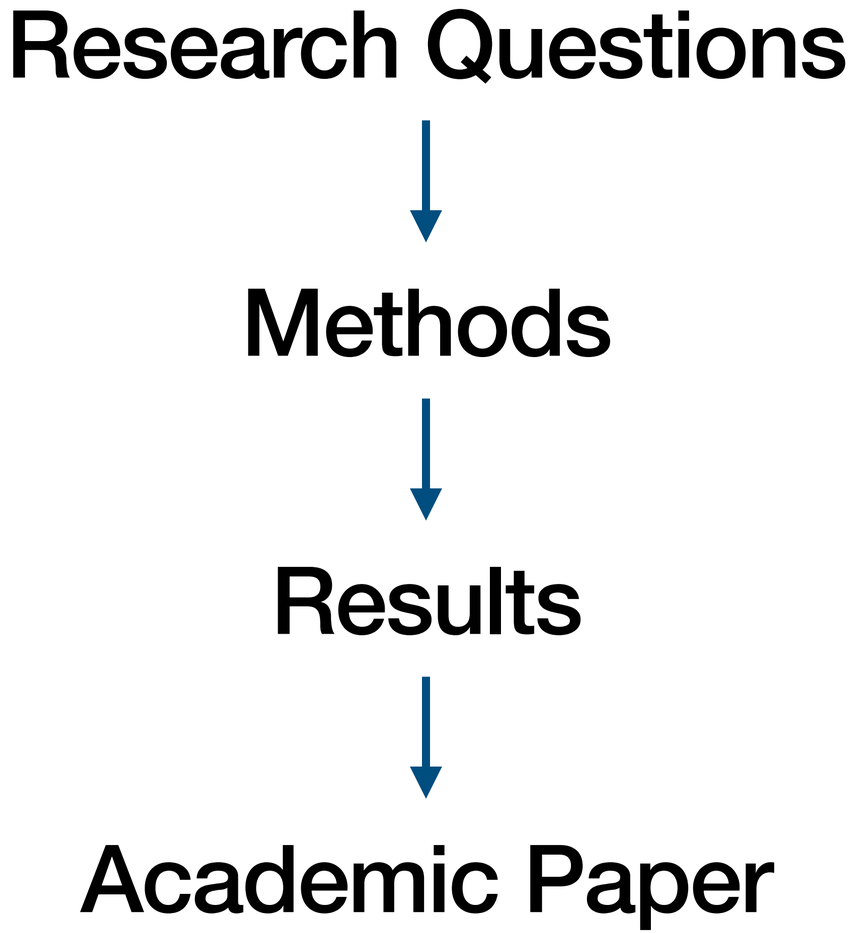
computer science researchers in senior policy roles in the entire Biden-Harris administration

…many/most in OSTP.

And if computer scientists aren’t involved, who is?

Part I
Why Computer Science Is Needed in Public Policy

Part II
How to Achieve Policy Impact with Computer Science


Research Questions
Methods
Results
Academic Paper

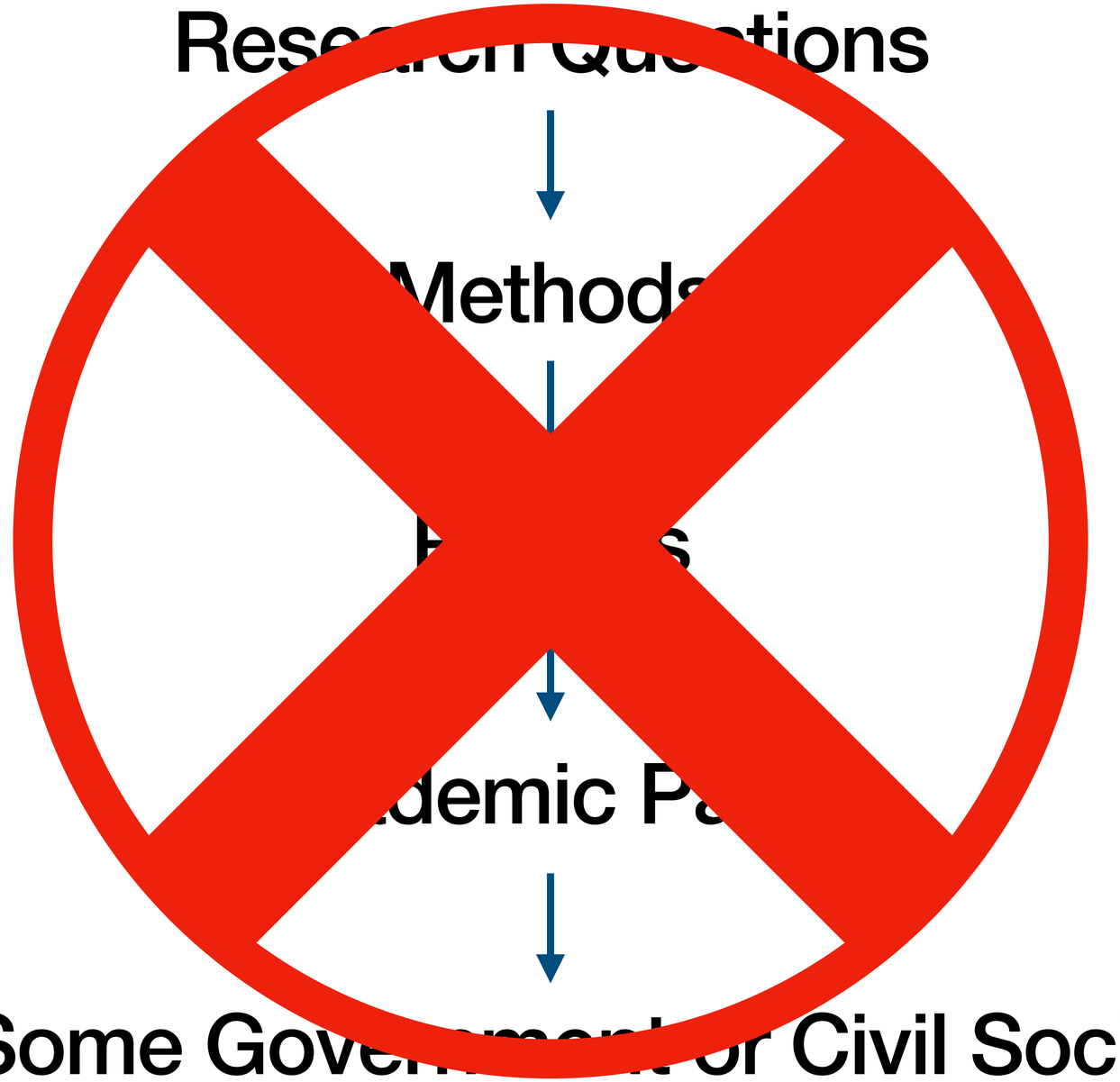
Research Questions

Methods

Results

Academic Paper

Go Talk to Some Government or Civil Society Person


Research Questions
Methods
Academic Pa
Go Talk to Some Government or Civil Society Person

Policy Context

↓

Research Questions

↓

Methods

↓

Results

↓

Academic Paper

↓

Policy Outputs

Policy Context

↓

Research Questions

↓

Methods

↓

Results

↓

Academic Paper

↓

Policy Outputs

Learn from Policy Practitioners

Learn from Affected People

Identify Opportunities for Impact

Develop a Theory of Change

Evaluate the Theory of Change

Computer science can create new capabilities
provide enforcement leads
change the solution space
highlight problems
provide facts & arguments
evaluate efficacy
call out BS
forecast developments
offer credibility
overcome partisanship
…

Policy Context

↓

Research Questions

↓

Methods

↓

Results

↓

Academic Paper

↓

Policy Outputs

Policymakers aren’t going to read your paper.*

Policy Context

↓

Research Questions

↓

Methods

↓

Results

↓

Academic Paper

↓

Policy Outputs

Briefings for Staff and Principals

Engagement with Civil Society

Administrative Comments

Enforcement Tips

Legislative Proposals

Testimony

General Audience Writing (e.g., Op-Eds)

Policy Context

↓

Research Questions

↓

Methods

↓

Results

↓

Academic Paper

↓

Policy Outputs

Persistence

Patience

An Empirical Study of Wireless Carrier Authentication for SIM Swaps

Kevin Lee Ben Kaiser Jonathan Mayer Arvind Narayanan

Department of Computer Science and Center for Information Technology Policy
Princeton University

Abstract

We examined the authentication procedures used by five prepaid wireless carriers when a customer attempted to change their SIM card. These procedures are an important line of defense against attackers who seek to hijack victims' phone numbers by posing as the victim and calling the carrier to request that service be transferred to a SIM card the attacker possesses. We found that all five carriers used insecure authentication challenges that could be easily subverted by attackers. We also found that attackers generally only needed to target the most vulnerable authentication challenges, because the rest could be bypassed. Authentication of SIM swap requests presents a classic usability-security trade-off, with carriers underemphasizing security. In an anecdotal evaluation of postpaid accounts at three carriers, presented in Appendix A, we also found—very tentatively—that some carriers may have implemented stronger authentication for postpaid accounts than for prepaid accounts.

To quantify the downstream effects of these vulnerabilities, we reverse-engineered the authentication policies of over 140 websites that offer phone-based authentication. We rated the level of vulnerability of users of each website to a SIM swap attack, and have released our findings as an annotated dataset on `issms2fasecure.com`. Notably, we found 17 websites on which user accounts can be compromised based on a SIM swap alone, i.e., without a password compromise. We encountered failures in vulnerability disclosure processes that resulted in these vulnerabilities remaining unfixed by nine of the 17 companies despite our responsible disclosure. Finally, we analyzed enterprise MFA solutions from three vendors, finding that two of them give users inadequate control over the security-usability tradeoff.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

1 Introduction

Mobile devices serve many purposes: communication, productivity, entertainment, and much more. In recent years, they have also come to be used for personal identity verification, especially by online services. This method involves sending a single-use passcode to a user's phone via an SMS text message or phone call, then prompting the user to provide that passcode at the point of authentication. Phone-based passcodes are frequently used as one of the authentication factors in a multi-factor authentication (MFA) scheme and as an account recovery mechanism.

To hijack accounts that are protected by phone-based passcode authentication, attackers attempt to intercept these passcodes. This can be done in a number of ways, including surveilling the target's mobile device or stealing the passcode with a phishing attack, but the most widely reported method for intercepting phone-based authentication passcodes is a SIM swap attack. By making an unauthorized change to the victim's mobile carrier account, the attacker diverts service, including calls and messages, to a new SIM card and device that they control.

SIM swap attacks allow attackers to intercept calls and messages, impersonate victims, and perform denial-of-service (DoS) attacks. They have been widely used to hack into social media accounts, steal cryptocurrencies, and break into bank accounts [1–3]. This vulnerability is severe and widely known; since 2016 NIST has distinguished SMS-based authentication from other out-of-band authentication methods due to heightened security risks including "SIM change" [4].

SIM swap procedures have valid purposes: for example, if a user has misplaced their original device or acquired a new device that uses a different size SIM card slot than the device it is replacing. In these cases, customers contact their carrier (often by calling the carriers' customer service line) to request a SIM card update on their account. The customer is then typically presented with a series of challenges that are used to authenticate them. If the customer is successfully authenticated, the customer service representative (CSR) proceeds to update the SIM card on the account as requested.

We examined the types of authentication mechanisms in place for such requests at five U.S. prepaid carriers——AT&T,

PRINCETON UNIVERSITY

CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

November 15, 2021

Federal Communications Commission
45 L Street NE
Washington, DC 20554

COMMENTS IN THE MATTER OF PROTECTING CONSUMERS FROM SIM SWAP AND PORT-OUT FRAUD
WC Docket No. 21-341

Thank you for the opportunity to provide comments on how the FCC can protect telecommunications customers from subscriber identity module (SIM) swap fraud, number port-out fraud, and related security and privacy threats.

We are academic researchers affiliated with the Center for Information Technology Policy (CITP) at Princeton University, one of whom previously served as Chief Technologist of the Commission's Enforcement Bureau. In a recent computer science publication, which the Commission references in the Notice of Proposed Rulemaking, we examined the SIM swap customer authentication practices of major U.S. wireless carriers.[1]

Our study involved a straightforward methodology. We created ten prepaid accounts at each of five carriers, then called customer service and attempted a SIM swap using limited information that might be available to an unsophisticated attacker. Our research methods enabled us to document the customer authentication process for each carrier.

We found pervasive insecurity. All five carriers used forms of customer authentication that are not generally accepted in the field of information security and that have serious security shortcomings. Carriers also did not have an apparent mechanism for responding to suspicious or failed authentication attempts—we were able to keep trying alternative modes of authentication, without notice to our simulated account owners. On several occasions, customer service representatives volunteered account information even though we had not successfully authenticated.

---

[1] Kevin Lee, Benjamin Kaiser, Jonathan Mayer & Arvind Narayanan, *An Empirical Study of Wireless Carrier Authentication for SIM Swaps*, Usenix Symposium on Usable Security and Privacy (Aug. 2020), *available at* https://www.usenix.org/system/files/soups2020-lee.pdf (attached as a copy for purposes of the rulemaking record).

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Consumers from SIM Swap and Port-Out Fraud	)	WC Docket No. 21-341
	)	

REPORT AND ORDER AND FURTHER NOTICE OF PROPOSED RULEMAKING

Adopted: November 15, 2023 **Released: November 16, 2023**

Comment Date: (30 days after Federal Register Publication)
Reply Comment Date: (60 days after Federal Register Publication)

By the Commission: Chairwoman Rosenworcel and Commissioners Starks and Gomez issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION

1. Today, we adopt measures designed to address two fraudulent practices bad actors use to take control of consumers' cell phone accounts and wreak havoc on people's financial and digital lives without ever gaining physical control of a consumer's phone. In the first type of scam, a bad actor

Identifying Harmful Media in End-to-End Encrypted Communication: Efficient Private Membership Computation

Anunay Kulshrestha
Princeton University

Jonathan Mayer
Princeton University

Abstract

End-to-end encryption (E2EE) poses a challenge for automated detection of harmful media, such as child sexual abuse material and extremist content. The predominant approach at present, perceptual hash matching, is not viable because in E2EE a communications service cannot access user content.

In this work, we explore the technical feasibility of privacy-preserving perceptual hash matching for E2EE services. We begin by formalizing the problem space and identifying fundamental limitations for protocols. Next, we evaluate the predictive performance of common perceptual hash functions to understand privacy risks to E2EE users and contextualize errors associated with the protocols we design.

Our primary contribution is a set of constructions for privacy-preserving perceptual hash matching. We design and evaluate client-side constructions for scenarios where disclosing the set of harmful hashes is acceptable. We then design and evaluate interactive protocols that optionally protect the hash set and do not disclose matches to users. The constructions that we propose are practical for deployment on mobile devices and introduce a limited additional risk of false negatives.

1 Introduction

The trend toward end-to-end encryption (E2EE) in popular messaging services [1], such as Apple iMessage [2], WhatsApp [3], Facebook Messenger [4], and Signal [5], has immense benefits. E2EE limits access to communications content to just the parties, providing a valuable defense against security threats, privacy risks, and—in some jurisdictions—illegitimate surveillance and other human rights abuses.

Adoption of E2EE does, however, come at a significant societal cost. A small proportion of users share harmful media, such as child sexual abuse material (CSAM), terrorist recruiting imagery, and most recently dangerous disinformation about causes of and cures for COVID-19 [6–9]. Present E2EE deployments do not support the predominant methods for automatically identifying this content.

For over a decade, popular platforms have relied on perceptual hash matching (PHM) to efficiently respond to harmful media [10]. PHM systems use perceptual hash functions (PHFs) to deterministically map media—most commonly images—to a space where proximity reflects perceptual similarity. PHFs are designed to be robust against common transformations, including geometric transformations, noise, and compression [11–19]. When a user shares media, a PHM system computes the perceptual hash and compares the value to a set of known hashes for harmful content. If the computed value is close to a hash in the set, the platform flags the user's media for a content moderation response.

In the United States, the National Center for Missing and Exploited Children (NCMEC) coordinates several datasets of known CSAM perceptual hashes, totaling millions of images [20, 21]. Similar CSAM hash clearinghouses exist in other countries, including the U.K. [22] and Canada [23]. The Global Internet Forum to Counter Terrorism (GIFCT), a coalition of technology firms, facilitates sharing tens of thousands of perceptual hashes for extremist material [24].

Because E2EE services by design do not have access to communications content, they cannot compute and compare perceptual hashes of user media. Law enforcement and civil society stakeholders worldwide have responded by pressing for a moratorium on E2EE adoption and "lawful access" schemes for encrypted communications [25–27].

In this work, we explore the technical feasibility of a middle ground: can an E2EE service take content moderation action against media that matches a perceptual hash set, without learning about non-harmful content, optionally without learning about harmful content, and optionally without disclosing the hash set? Our contributions to the literature, and the structure of the paper, are as follows:

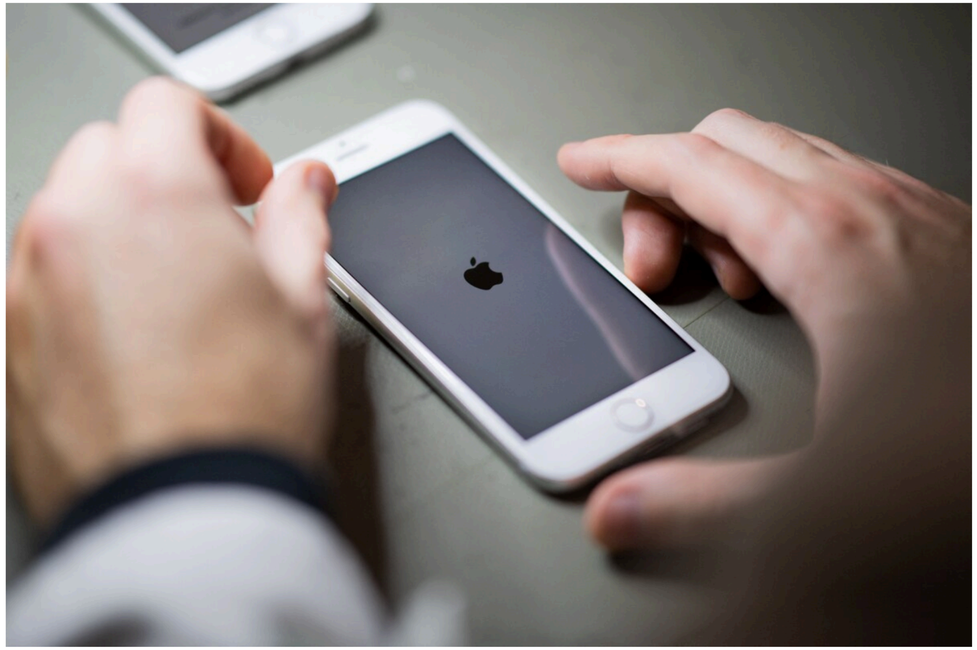
- We formalize the problem of detecting perceptual hash matches in E2EE communications: private exact membership computation (PEMC) and private approximate membership computation (PAMC). We also describe limitations in the problem formulation, including both technical constraints and serious policy concerns that cannot be resolved through technical means (Section 2).
- We evaluate commonly used PHFs for predictive performance, so that we can both characterize the added privacy risk to E2EE communications from PHM false positives and contextualize the additional false negatives associated with certain of our protocol designs (Section 4).
- We evaluate client-side PEMC and PAMC designs, which are straightforward and practical for deployments where the set of perceptual hashes is not sensitive (Section 5).
- We design and evaluate novel interactive protocols for PEMC and PAMC (Section 6). Our protocols consist of four steps: bucketizing PHF values for efficient lookup

Opinion

We built a system like Apple's to flag child sexual abuse material — and concluded the tech was dangerous

August 19, 2021

421



An employee reconditions an iPhone in Sainte-Luce-sur-Loire, France, on Jan. 26. (Loic Venance/AFP/Getty Images)

By Jonathan Mayer and Anunay Kulshrestha

Estimating Incidental Collection in Foreign Intelligence Surveillance: Large-Scale Multiparty Private Set Intersection with Union and Sum

Anunay Kulshrestha
Princeton University

Jonathan Mayer
Princeton University

Abstract

Section 702 of the Foreign Intelligence Surveillance Act authorizes U.S. intelligence agencies to intercept communications content without obtaining a warrant. While Section 702 requires targeting foreigners abroad for intelligence purposes, agencies "incidentally" collect communications to or from Americans and can search that data for purposes beyond intelligence gathering. For over a decade, members of Congress and civil society organizations have called on the U.S. Intelligence Community (IC) to estimate the scale of incidental collection. Senior intelligence officials have acknowledged the value of quantitative transparency for incidental collection, but the IC has not identified a satisfactory estimation method that respects individual privacy, protects intelligence sources and methods, and imposes minimal burden on IC resources.

In this work, we propose a novel approach to estimating incidental collection using secure multiparty computation (MPC). The IC possesses records about the parties to intercepted communications, and communications services possess country-level location for users. By combining these datasets with MPC, it is possible to generate an automated aggregate estimate of incidental collection that maintains confidentiality for intercepted communications and user locations.

We formalize our proposal as a new variant of private set intersection, which we term multiparty private set intersection with union and sum (MPSIU-Sum). We then design and evaluate an efficient MPSIU-Sum protocol, based on elliptic curve cryptography and partially homomorphic encryption. Our protocol performs well at the large scale necessary for estimating incidental collection in Section 702 surveillance.

1 Introduction

When a nation conducts surveillance directed outside its own borders and at foreign intelligence targets, how often does it intercept communications involving its own people? For over a decade, that seemingly simple factual question has been a flashpoint in United States national security law.

Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorizes agencies in the U.S. Intelligence Community (IC) to collect communications inside the U.S. when targeting foreigners abroad [2, 36, 62]. Section 702, unlike conventional law enforcement and FISA procedures for obtaining communications content, does not require applying to a court for a warrant demonstrating probable cause and particularity for a specific target. Instead, the IC obtains annual program approvals from the Foreign Intelligence Surveillance Court (FISC), then directs communications services in the U.S. to facilitate surveillance of foreign intelligence targets.

The structure and implementation of Section 702 have prompted significant controversy, especially over "incidental" collection of communications to and from U.S. citizens and other persons protected by constitutional privacy guarantees. The statutory framework and FISC orders permit agencies to query and use these communications for purposes beyond foreign intelligence, without obtaining a warrant as ordinarily required by the Fourth Amendment to the U.S. Constitution.

For over a decade, members of Congress (on a bipartisan basis) and civil society groups have repeatedly urged the IC to estimate the scale of incidental collection [5, 7, 8, 11, 14–18]. The IC's leadership has acknowledged the importance of an empirical estimate for public transparency [6, 9, 10, 12, 21]. Because the IC often lacks information about non-target parties to intercepted communications, however, it cannot readily compute an estimate. After years of exploring estimation methods, the IC has not identified a method that it considers adequate for respecting individual privacy, protecting intelligence sources and methods, and avoiding burdensome manual analysis. Section 2 provides further detail on Section 702 of FISA, incidental collection, and the estimation challenge.

In this work, we propose a novel path forward for estimating incidental collection using secure multiparty computation (MPC). The IC possesses records of the parties to intercepted communications, but may know little about non-target parties. Communications services possess country-level user location for business purposes, but may know little about intercepted communications. By combining these datasets with MPC, it

THE

PRIVACY AND CIVIL LIBERTIES

OVERSIGHT BOARD

REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

SEPTEMBER 28, 2023

Common Misstep 1

Research “about” a policy issue.

Common Misstep 2

Measuring what’s easily measurable.

Common Misstep 3

Getting the law or policy wrong or missing nuance.

Common Misstep 4

Trying to remain artificially “neutral.”

Uncommon Misstep

Filing in the wrong docket.

Part II
How to Achieve Policy Impact with Computer Science

Part III
Why Computer Science Isn’t Achieving Policy Impact

Computer science, as a discipline,
is failing society.

Example: AI/ML fairness and bias research

Teaching and Training

Hiring and Tenure Criteria

Publication Venues

Paper Review

Funding Opportunities

Paper, Thesis, and Career Awards

Leave Policies

Teaching and Training	Mandatory ethics classes?
Hiring and Tenure Criteria	Opportunity cost and timelines
Publication Venues	Shoehorning? ACM CS + Law?
Paper Review	Emphasis on technical novelty
Funding Opportunities	Broader Impacts? NSF DASS?
Paper, Thesis, and Career Awards	Privacy Papers for Policymakers?
Leave Policies	Research and Industry Favored

Teaching and Training	Courses and opportunities
Hiring and Tenure Criteria	Policy is a plus or primary factor
Publication Venues	Add policy to conference scope
Paper Review	State acceptance criteria
Funding Opportunities	Reboot
Paper, Thesis, and Career Awards	Start some!
Leave Policies	Encourage public service

Other disciplines have figured this out!

Examples: economics and law

Public policy should be a recognized field within the discipline of computer science.

Part III
Why Computer Science Isn’t Achieving Policy Impact

Policy Impact with Computer Science

Why It's Needed,
How to Achieve It, and
Why We Don't

Jonathan Mayer
Princeton University
July 14, 2025