Content Moderation on End-to-End Encrypted Systems

Charles Duan
James Grimmelmann

Computer Science and the Law Roundtable
May 23, 2023

E2EE MESSAGING

CONTENT MODERATION

ROUND 812

Message Franking
Forward Tracing
Homomorphic Encryption

E2EE Messaging

Content Moderation

imgflip.com

Content moderation technologies for E2EE

- Message franking
- Forward tracing
- Client-side scanning
- Sever-side scanning

Communications Privacy Laws

- Wiretap Act (WA)
- Stored Communications Act (SCA)
- Pen Register Act (PRA)
- Communications Assistance for Law Enforcement Act (CALEA)
- Computer Fraud and Abuse Act (CFAA)

In the paper

	Wiretap Act	SCA	PRA	CALEA	CFAA
Message Franking					
Forward Tracing					
Client-Side Scanning					
Server-Side Scanning					

In this talk

	Wiretap Act
Message Franking	

Zooming In

Wiretap Act

- "any person who …intentionally intercepts … any … electronic communication … shall be punished." 18 U.S.C. § 2511(1)(a)
- "'intercept' means … acquisition of the contents of any … electronic … communication through the use of any … device." *Id.* § 2510(4)
- "'contents' … includes any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8)

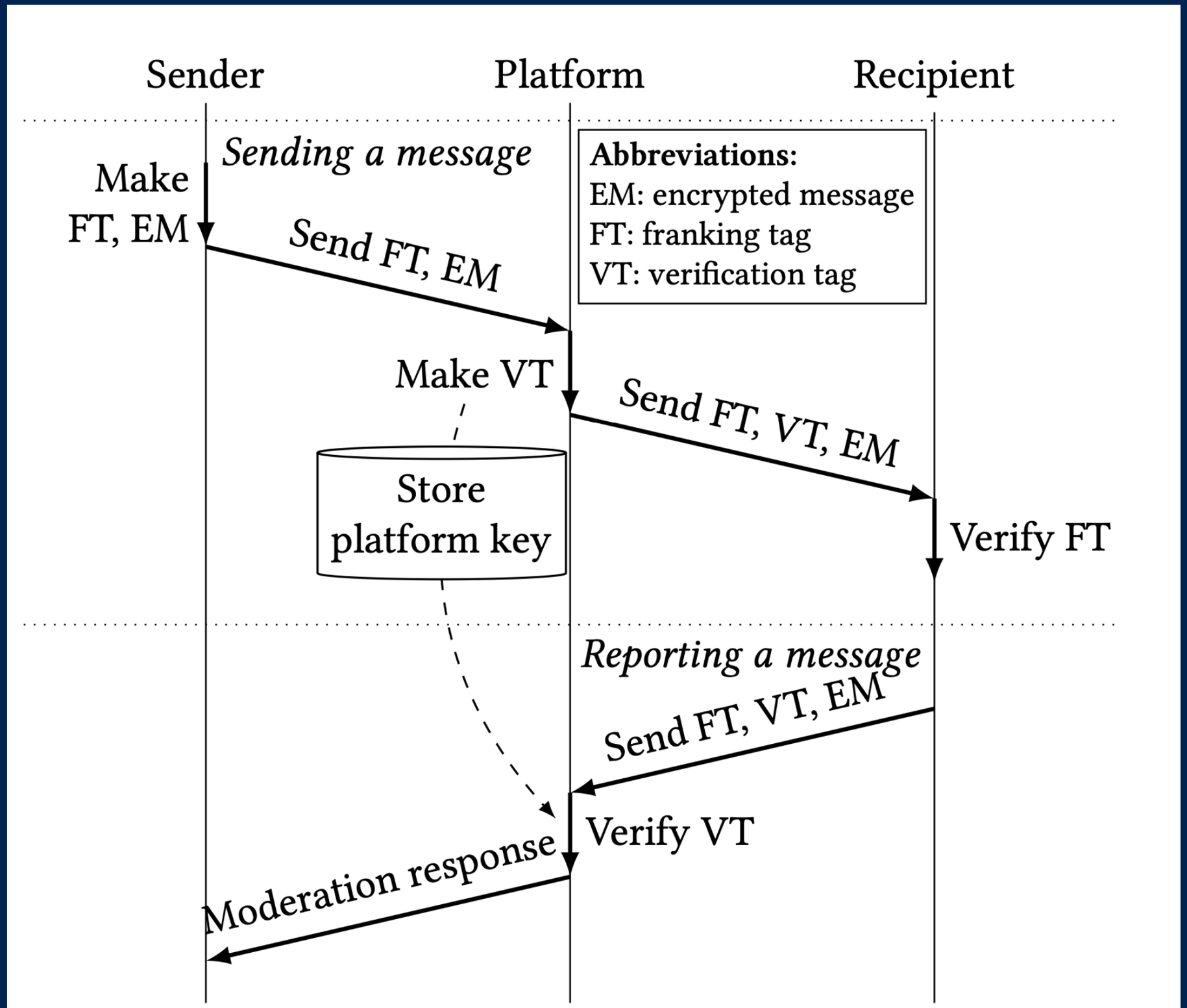
Wiretap Act elements

1. intentional
2. interception
3. of the contents
4. of an electronic communication
5. using a device

Wiretap Act exceptions

- "where such person is a party to the communication" 18 U.S.C. § 2511(2)(d)
- "where one of the parties to the communication has given prior consent." *Id*.
- "by a provider … in the ordinary course of its business." *Id*. § 2510(5)(a)(ii)
- "any activity which is a necessary incident to the rendition of … service." *Id*. § 2511(2)(a)

Message franking



Legal issues

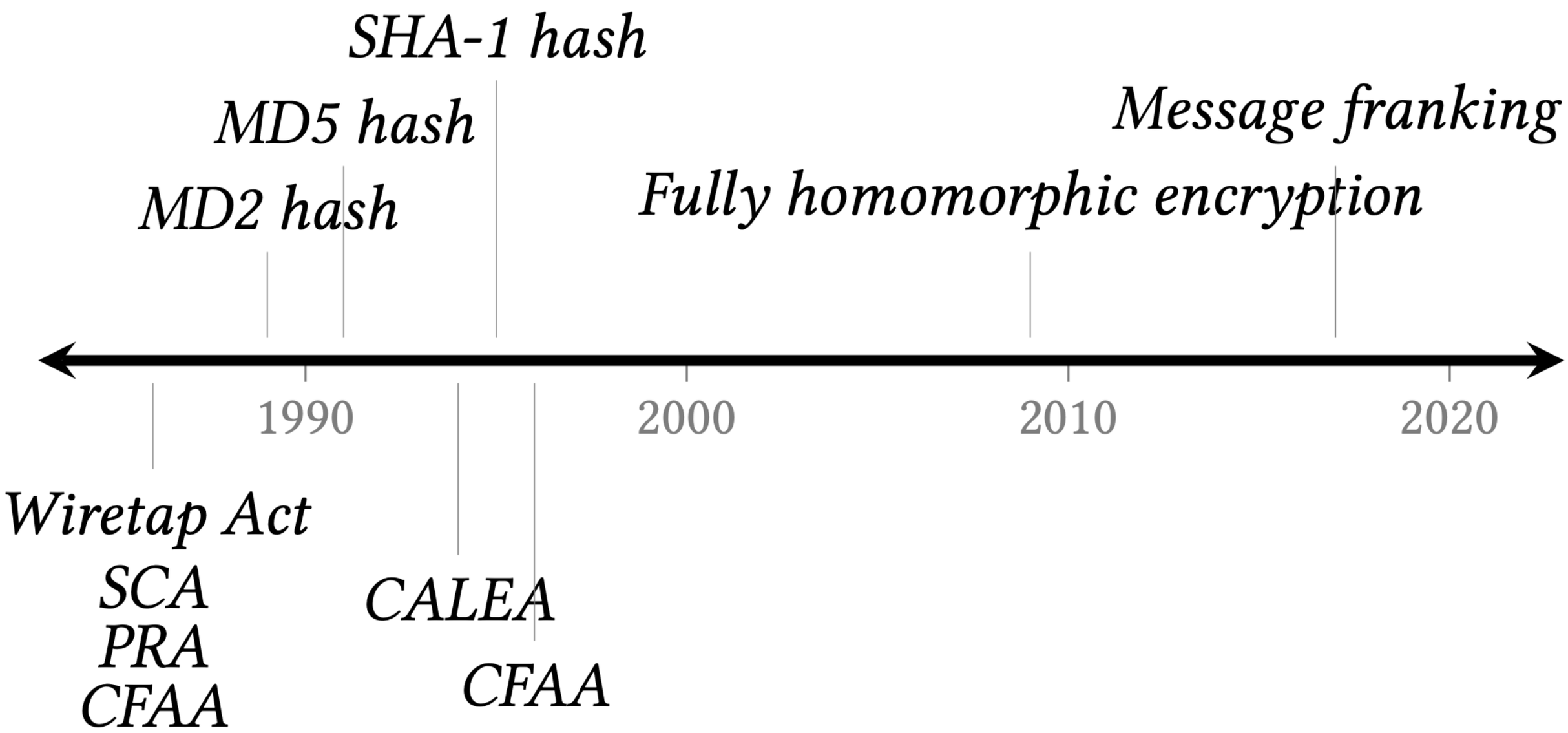
- Is a cryptographic hash “contents”?
- Do the users “consent” to the franking protocol?
- Is the platform a “party” to the communication?
- Is message franking “in the ordinary course” of the platform’s business?

So is it legal?

- Message franking is *probably* legal …
  - … but not *definitely* legal
- This seems like the kind of question that ought to have an unambiguous answer

Zooming Out

Timeline


SHA-1 hash
MD5 hash
MD2 hash
Message franking
Fully homomorphic encryption
1990
2000
2010
2020
Wiretap Act
SCA
PRA
CFAA
CALEA
CFAA

Broader lessons

- There are about a dozen boxes in our table that are equally complex and interesting
- Communications privacy law needs an update
- So what should we fix?

Inartful variation: contents vs. metadata

- WA: “contents”
- SCA: “contents” vs. “records of session times and duration”
- PRA: “contents” vs. “dialing, routing, addressing, or signaling information”
- CALEA: “contents” vs. “call- identifying information”
- CFAA: “information”

Common questions

- What kinds of information are protected?
- What kinds of devices are covered?
- What counts as valid consent?
- What is a valid business purpose?
- *What is "end-to-end encryption"?*

Discussion