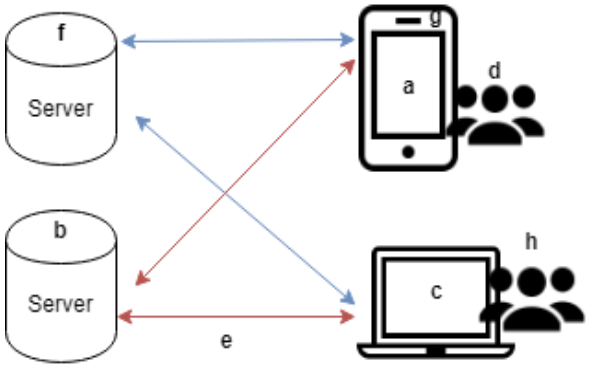
Visual Content Privacy Leaks on Social Media Networks

With the growth and accessibility of mobile devices and internet, the ease of posting and sharing content on social media networks (SMNs) has increased exponentially. Many users post images that contain "privacy leaks" regarding themselves or someone else. The Hawaii Emergency Agency example provides evidence that visual content privacy leaks can happen on an individual or organization level.

MITIGATION TECHNIQUES



a	Client side
b	Privacy Patrol
c	Chaperone Bot
d	Category tag
e	Privacy Score
f	Server Side
g	Interception
h	Redaction

Location

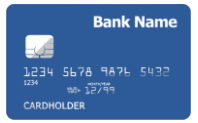
An attacker can use this vector to find out where an individual lives and/or current location.

Identity

An attacker can use this vector to exploit an individual's identity, even to the very intimate details.

Asset

An attacker can use this vector to exploit an individual's possessions and valuables.



REDACTION TECHNIQUES

We have 5 techniques in our redaction spectrum, we believe that technique four will bring a significant contribution to typical user's of SMNs. The fourth option is to use adversarial noise. We believe that adversarial noise will be important feature added to visual content to help protect SMNs user from computer attacks. By adding a few pixels, we could

(1) impede their ability to learn anything from the visual content even if it is in their possession

(2) still allow the images to be visible to humans.