Technical Disclosure Commons

Defensive Publications Series

October 2019

Warning Mobile Device Camera Users of Potential Dangers

N/A

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
N/A, "Warning Mobile Device Camera Users of Potential Dangers", Technical Disclosure Commons, (October 22, 2019)
https://www.tdcommons.org/dpubs_series/2591

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Warning Mobile Device Camera Users of Potential Dangers

Abstract:

This publication describes methods of warning a user of a mobile device camera application of potentially dangerous locations and situations. In aspects, a danger warning manager on the mobile device acquires context signals (*e.g.*, captured images, global navigation satellite system location information, social media history for a location) and analyzes these context signals to determine a level of risk. Upon determining that the user is potentially in danger, the danger warning manager causes the mobile device to present warning notifications to the user.

Keywords:

Photography, image, image capturing device, camera, machine-learned (ML) model, social media, dangerous, selfie, geolocation, GNSS, GPS, safety, smartphone

Background:

Social media platforms, particularly photo-oriented social networks, frequently display awe-inspiring and dramatic photographs and videos (collectively "images") posted by social media users in dangerous situations. For example, a social media user, such as an influential social media user ("influencer"), may post images of themselves buildering (climbing) the outside of a building, standing close to a precipice, or taking a self-portrait digital photograph ("selfie") with wildlife.

Frequently, mobile device users attempt to recreate such images, particularly those posted by social media influencers, without appreciating the potential risks involved in taking such images. During the process of recreating such an image, a mobile device user will visit a

notoriously dangerous location and will likely take a number of photographs, attempting to get a perfect "shot."

In an effort to prevent users from harm, it is desirable for mobile devices to acquire contextual signals (*e.g.*, geolocation, content of previous images, social media history related to the geolocation, social media accounts followed by the user, user actions), evaluate risk, and present a warning that may notify a mobile device user of unanticipated danger.

Description:

This publication describes methods, implemented on a mobile device, of determining potentially hazardous situations and warning a mobile device camera application user of the potential danger. An exemplary mobile device, such as a smartphone, includes a display, sensors (*e.g.*, a camera, a global navigation satellite system (GNSS) location sensor), a haptic mechanism, a speaker, a processor, and a computer-readable medium (CRM). The CRM may include the operating system of the mobile device, a camera application, and a danger warning manager (DWM).

In some aspects, context signals are received, determined, collected, and/or measured by the mobile device. Examples of context signals include the content of previous images captured by the user, the number of images captured by the user in a short period of time, the location of the mobile device (*e.g.*, from a GNSS location sensor), social media history related to the location (*e.g.*, whether an influencer took a selfie at the location), a risk history for the location (*e.g.*, whether the location is known to be potentially dangerous, known to frequently have dangerous wildlife present, known to have climbing hazards, known to have cliff hazards), social media accounts followed by the mobile device user, and sequences of actions taken by the user.

Context signals may be provided as inputs to a machine-learned (ML) model. The ML model may be iteratively trained, off-device, to analyze inputted context signals and estimate risk. After sufficient training, the ML model can be deployed to the CRM of the mobile device. When implemented on a mobile device, context signals can be provided as inputs to the ML model, and the ML model can estimate risk. In aspects, the ML model can be trained to perform object detection on images to determine the presence of dangerous objects (*e.g.*, wildlife).

Figure 1, below, illustrates an example of how a ML model may analyze a context signal and estimate a risk level.

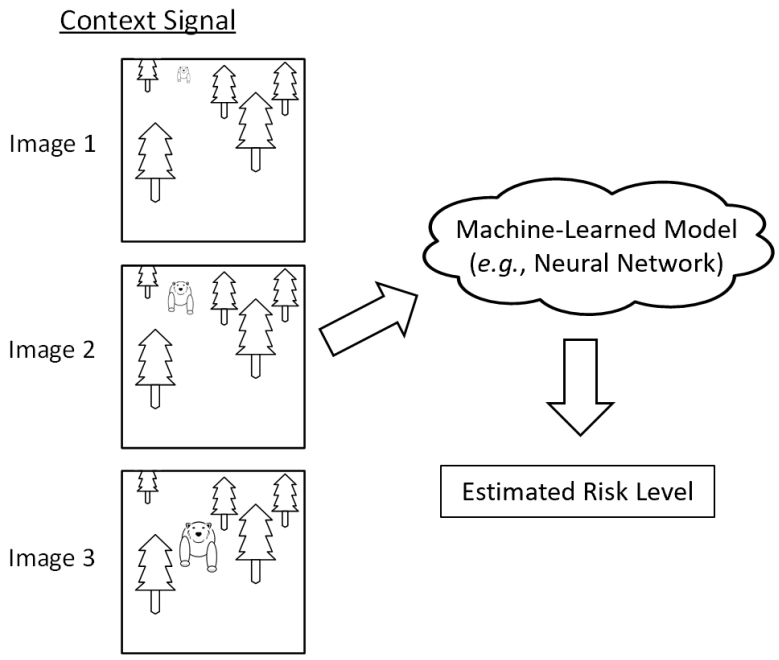

Figure 1

As illustrated in Figure 1, the context signal is a sequence of images taken by the user using a camera application of a mobile device. The images are of outdoor scenes. Geolocation data for the device and the images are provided as inputs to a ML model. The ML model analyzes the geolocation data to determine a location history. The ML model analyzes the images, detects an

object, determines that the object is an animal (bear), and determines that the animal is moving closer to the user.

Based on such information, the ML model estimates a risk level for the situation. The estimated risk level may be determined through estimates from one or more ML models. In other words, ancillary risk level estimates can alter the total risk level estimate. For example, a ML model may analyze a context signal and estimate a risk level similar to Figure 1 (*e.g.*, the animal is moving closer to the user), while another ML model may receive a context signal that contains geolocation information indicating that the user is at a zoo. As a result, the ML model could estimate a low-risk level and decrease the total estimated risk level. Conversely, if the input to the ML model indicates that the location is well-known for frequently having dangerous wildlife present, then the total estimated risk level would increase.

In a third step, if the total estimated risk level outputted by the ML model exceeds safe condition levels, then the DWM can trigger a haptic mechanism on the mobile device to vibrate, trigger a sound to be emitted from a speaker of the mobile device, and/or present a notification on the display of the mobile device. The notification can present facts and statistics about the risk of capturing such an image, in an effort to dissuade the user from continuing the risky behavior. The notification may further ask the user for input (*e.g.*, confirmation that the user has seen the warning).

In another example instance, a user (Jane) is hiking on Mount Hua in China and is using the camera application on her mobile device to take photographs. The ML model analyzes context signals including: geolocation data relating to Jane's location, the number of photographs taken by Jane in a short amount of time, information (including geolocation data) that a social media influencer recently took a selfie image on a dangerous cliff on Mount Hua, and information

indicating that Jane follows the social media influencer. Based on this information, the ML model estimates a risk level. Upon determining that Jane may be attempting to recreate the social media influencer's selfie image, the DWM of the mobile device may provide a notification to Jane warning her of the danger of taking a selfie on the dangerous cliff.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs, or features described herein may enable collection of user information (*e.g.*, information about a user's social network, social actions, social activities, profession, a user's preferences, a user's geolocation), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

In summary, to prevent users from harm it is desirable for mobile devices to acquire contextual signals (*e.g.*, geolocation, content of previous images, social media history related to the geolocation, social media accounts followed by the user, user actions), evaluate risk, and present a warning that may notify a mobile device user of unanticipated danger.