INKSCREEN

PHOTOS ARE WORTH 1,000 CUTS

HOW INKSCREEN CAN LIMIT THE DAMAGE

Beginning with the first crude drawing painted in a Neolithic cave, people have understood the intrinsic value of pictures. Long before a marketeer coined the phrase “a picture is worth a thousand words” others understood the power of pictures to convey more meaning than a verbal description. No matter how well written, words cannot satisfactorily capture the beauty of a sunset or a Mona Lisa smile. Leonardo da Vinci wrote a poet would essentially go crazy trying to put into words what a painter can express in an instant.

Created by Charles Kolodgy of Security Mindsets

This ability to instantly capture information is ultimately why cameras and the applications that utilize them have become desired mobile phone features. Mobile phones are a key tool for employee productivity and their use will continue. The types of phones, who owns them, and how they are used vary from organization to organization. The use of these tools, which conveys considerable information or provides a portal into an organization's systems, puts a target on them. Attackers and cyber criminals attack mobile phones in order to exploit them for ill-gotten gains.

Companies are aware mobile phones have vulnerabilities and take precautions to protect themselves from damage. One activity difficult to control is the use of the camera. Most mobile device security products have not been able to address this area. This short paper highlights this issue and offers up a solution which improves security, supports mobile device management, and enhances compliance.

MOBILE CAMERAS—THE EYE OF THE MACHINE

People have long been interested in preserving what they see. First it was drawings and paintings and eventually photography was developed. For over 170 years people have been taking pictures. Technological improvements make picture taking and video capture easy. So simple that Keypoint Intelligence estimated that 1.4 trillion pictures would be snapped in 2020 with 90% of those being created by a smartphone.[1]

Digital photography grew out of research supporting military, scientific, and medical applications. Commercial digital cameras first appeared in the late 1980s. The first cellular phone with a camera was released in 1999. Having both phone and camera readily available appeals to many. By 2007 when Apple released the iPhone, an integrated digital camera was an indispensable component for smart phones. Mobile phones now do not just have one camera but multiple cameras with increasing resolution, additional functionality, and photo quality. Phone camera image processing is constantly improving. The use of artificial intelligence-based computation is used to enhance pictures, improve lighting conditions, and offer 3D sensing capabilities.

The quality of mobile phone cameras has improved and the computational power of smartphones and storage has increased to the point that many people no longer carry or buy a dedicated camera. The advanced imaging capabilities imbedded in a smart mobile device also allows for much greater functionality. Activities previously requiring real-time pictures taken with a standalone camera or specialty equipment have been replaced by mobile phone digital cameras. These developments have resulted in camera shipments declining by 87% between 2010 and 2019 as reported by the Camera & Imaging Products Association.[2]

1 How Many Photos Will Be Taken in 2020. (2020, January 10) Life in Focus. Retrieved March 18, 2021 from https://focus.mylio.com/tech-today/how-many-photos-will-be-taken-in-2020

2 Richter, Felix. (2020, December 9). *Smartphones Wipe Out 40 Years of Camera Industry Growth*. Statista. https://www.statista.com/chart/15524/worldwide-camera-shipments/

The power of a mobile camera isn't specifically its photographic functionality but is measured by how applications can leverage the camera functionality or images the camera generates. There are innumerable task that can be performed using the advanced capabilities of a phone's camera coupled with an application. For over a decade apps have continuously expanded how they utilize mobile phone cameras to capture, share, process, and store imaging data. Initially mobile phone photos and videos were primarily for sharing with others using messaging, email, social media, and uploaded to online storage. Now there are innumerable business uses, which is why the mobile phone has become indispensable as a productivity tool.

USE CASES—I CAN DO THAT WITH MY PHONE!

Cameras are designed to take pictures. What you do with those images and videos are what makes them special and ultimately valuable. For most consumers pictures and videos are designed to distribute and to save. They are used to remember memories or to share events. Given that people can immediately snap pictures and have them readily available the phone camera acts as a quick reminder tool.

The sharing of photos and use of them to convey information is not limited to individuals. Businesses have found these tasks useful. Research shows there is a 34% increase in productivity when employees are allowed to use mobile devices for work. Employees capture meeting notes or document workflow processes.[3] Pictures of information are texted or emailed to colleagues for immediate feedback or action. Companies, especially smaller companies, use phone snapshots in business blogs and presentations to enhance their message. Insurance adjusters use mobile phone photos to document damage for claims settlement. Home medical staff provide pictures and video to doctors for quick diagnosis. Home healthcare applications also use the camera to take heart rate, blood pressure, and provide simple lab results. These activities are simple but more complex applications are available.

A number of applications use the camera on a smartphone as an input devices. These include a language translation, document scanning, picture-based searching, location determination, biometric recognition, scan QR (Quick Response) codes, and remote check depositing. Many of these activities are considered commonplace. Applications which utilize a phone's camera are constantly being developed and improved. For example QR codes are generally used to directly connect to a website. Advances in the technology are being developed which utilize QR codes as an authenticator.

Businesses are increasingly using smartphone cameras as all-purpose sensors for harvesting data. With a smartphone and appropriate applications a smartphone can become a virtual office. The ability to be productive remotely has been extremely valuable over the past year as work from home became a norm for many organizations.

MOBILE PHONE CAMERA USES

Take Pictures

Share Pictures

Scan Documents

Character Recognition

Deposit Checks

Activate QRCodes

3 Tukek, Melanie. (2016, August 3). *Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research*, Insights. https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/#

Probably the most useful phone camera application for businesses is Optical Character Recognition (OCR). Digital scanning with a smartphone is easy and offers excellent text-recognition capabilities. Most OCR applications offer custom file management and automatic uploading to cloud storage.

Optical Character Recognition (OCR)

OCR technology converts handwritten, typed, scanned text, and text inside images to machine-readable information. This allows for digitized text to be easily presented, edited, searched, and saved. OCR allow for the sharing of all forms of data, both structured and unstructured. Using a phone's camera allows the passing of approval signatures quickly. Complete OCR programs use machine learning to improve text recognition accuracy, optimizes file and folder operations, and automated cloud storage.

It is interesting to note that many applications are considering using the smartphone camera for authentication purposes. Those can be via biometric face recognition, QR codes, and OCR based identity verification. For the latter operations people just display an ID card in front of the camera or upload the image. OCR technology does the rest.

The positives associated with the phone camera and its applications is growing in importance. However there are two sides to every coin. People concerned about security and data protection will wonder how this data is being protected and what threats it could hold for the organization.

WHAT IS HIDDEN BEHIND DIGITAL PHOTOS

The literal hidden aspect of digital photography is that the photos contain buried information. This metadata, as defined by the Exchangeable Image File Format (EXIF), is appended to each photo. This is similar to writing on the back of a physical photo. The EXIF metadata contains technical camera settings (such as exposure, light, shutter speed, and more), a thumbnail picture, and other details. At a deeper level, the metadata includes when and where a photo was taken. A phone's built-in GPS receiver appends location information in the EXIF header. These details embedded in every photo file. travels with the photo. When the picture is sent via email or posted online that information also goes with it.

The EXIF metadata information is useful. It allows for the sorting of pictures by date and location as well as identifying the origins of the content. The thumbnail allows for the

previewing of the picture on the camera's screen, file manager, and photo manipulation software. Although the data is purposeful, it also can pose a privacy problem, especially the location information, which is referred to as Geotagging.

> *Geotagging automatically attaches geographic locational information to images, video, and other media recorded by smartphones. The data generally consists of latitude and longitude coordinates but can also include altitude and bearing (distance from North).*

With this information cybercriminals or others can gain insight that can lead to physical threats or identity theft. From a business perspective, geolocation data presents a unique risk. Reviewing date and location data on pictures of executives or other officials could provide useful intelligence. It might be possible to guess about a merger, acquisition, or research breakthrough. The business could also utilize geolocation data to track employees' activities. There may be a justifiable business reasons for such monitoring but it is definitely a gray area.

Metadata including geotagging information is a potential vulnerability but it is only one of issues associated with smartphone digital cameras.

THREATS AND VULNERABILITIES FROM MOBILE DEVICE CAMERAS

Technology advances can make what was suspicious commonplace. There was a time when carrying a small, concealed camera would be problematic. People caught with a "spy" camera were generally espionage agents. Christopher Boyce and Andrew Daulton Lee, infamous spies better known as the Falcon and the Snowman, were discovered when a roll of microfilm taken using a miniature camera provided by the Soviets was found in Lee's possession. People now constantly carry a miniature camera as part of their smartphone. The ability to take pictures at any time is readily available.

I Spy With My Phone

Camera phones allow near immediate surveillance or data loss since the data capture tool is always present. It is relatively easy to discreetly take photographs or videos in museums, corporate offices, performance halls, factory floors, hospitals, or any place where photography is generally prohibited. Unlike the ancient physical spy cameras of old, today's network connected phone cameras allow for instantaneous remote storage. When a camera is misused these activities could result in privacy violations, copyright infringement, loss of proprietary information, or industrial espionage.

In addition to the privacy, compliance, and data loss issues related to mobile device photos, attackers can turn a smartphone into a clandestine monitoring device. Phone operating system vulnerabilities and malicious applications are a risk. With the large variety in phone models and thousands of applications it is difficult to know with certainty if a phone's camera is secretly being accessed. What has been demonstrated is the capability does exist. Researchers at the Naval Surface Warfare Center and Indiana University, in 2012 created PlaceRaider. The malware app remotely exploited an Android cell phone's camera to secretly snap a picture every two seconds. The photos can be uploaded thus allowing an attacker to perform remote reconnaissance.[4]

Yes It Can Happen—Phone Camera HiJacking

In November 2019 it was announced that several vulnerabilities in the Android OS would make it trivial to bypass restrictions on the use of a phone's hardware components. For an application to use the camera or microphone explicit user permission is required. The vulnerabilities uncovered by security firm Checkmarx allowed for an app to take pictures and record video and audio without user approval.[5] The secretly collected content, along with any other image or video stored on the device, could be sent to an attacker-controlled server. Retrieving the data would not be a hurdle for the remote attackers because permission to access storage is a commonly granted access right. The specific vulnerabilities, tracked as CVE-2019-2234, have been patched but others may still exist.

The bottom line is threats and vulnerabilities associated with the digital cameras exist. There are many ways they can be used against an organization. People use what could be defined as a secret spy device. It can facilitate data loss and lead to legal and regulatory compliance problems. The data contained within metadata offers hidden insight. Malware can exist within applications that access the camera and hackers can hijack the camera. Lastly, and possibly the greatest overall threat is digital photographs potentially exist in many locations. People have them on their phones, can store them in a personal cloud, share them using many communications platforms, and store them in public cloud repositories. This captured content can drift, either maliciously or inadvertently, unprotected outside the corporate sphere of influence and control.

REGAINING VISIBILITY AND CONTROL

Over the years organizations have deployed various types of mobile security. The emphasis has centered upon controlling access to devices, managing the security of the devices, limiting application deployment, checking for malware, encrypting data, and a number of other security functions. With all of these protective capabilities it is

4 DesMarais, Christina. (2012, September 12). *PlaceRaider app lets phone camera spy on people*. PCWorld. https://www.pcworld.com/article/2010860/PlaceRaider-app-lets-phone-camera-spy-on-people.html

5 Goodin, Dan. (2019, November 19). *Google & Samsung fix Android spying flow. Other makers may still be vulnerable*. Ars Technica. https://arstechnica.com/information-technology/2019/11/google-samsung-fix-android-spying-flaw-other-makers-may-still-be-vulnerable/

amazing that one area has been overlooked. **Many security controls are not able to manage or handle unstructured data created by a mobile phone's camera.** This is itself a risk organizations must address.

It is clear mobile device cameras are both a boon and a bane. For phone camera use to be a positive experience, it requires monitoring and controlling the flow of content. Organizations must assess how they safeguard the data generated by a smartphone, including images and information snapped by the camera. Content on mobile devices must be protected and managed across the entire content life cycle—from capturing, retaining, sharing, and uploading files.

Ensuring this level of data protection is difficult but necessary. Scanned documents and captured images and videos have become critical to business processes. To manage this companies need to establish policies that dictate what end users and their mobile devices can and cannot do with that content. Setting policy is great but enforcement is better.

Secure Content Capture

Secure Content Capture defines the types of controls organizations should be utilizing to provide visibility and control of information originating with a mobile device's camera. Below are the features enterprises should consider when looking at solutions dealing with camera image data protection.

Camera Functions:

- **Photos**: Capture high-resolution photos, apply annotations, add captions, and watermarks, to facilitate data management.
- **OCR**: Scan multi-page paper documents, convert them to readable text and save in standard data formats. Function must occur on device.
- **Videos**: Record, edit and apply "credits" to high-quality videos.
- **QR**: Scan QR codes, verify validity, and launch a secure browser for safe execution.

Data Management Functions:

- **Metadata**: Automatically annotate metadata to include username, time/date, location, and notes. Provide for visible stamping ("watermarking") on the media.
- **Data Isolation**: Separate business and personal media and files; business files can be wiped without impacting personal privacy. This is critical for organizations with Bring-Your-Own-Device (BYOD) or Corporate-Owned-Personally-Enabled (COPE) mobile management policies.
- **Encrypted Data Container**: Protect sensitive data residing on devices and in transit while also preventing access to content on lost/stolen devices.

CAPTOR™
by
INKSCREEN

PHOTOS
Take photos, apply annotations add captions and watermarks, manage metadata. Share as JPG or multi-page PDG.

DOCUMENTS
Scan paper documents, open and manage documents, combine PDFs. Apply e-signature and annotations (highlighter, notes, arrows, drawings).

VIDEO
Capture high resolution video with professional settings (ex. FPS, recording quality). Apply "final frame" credits. Extract transcript. Share as MP4

AUDIO
Record ambient audio (ex. depositions, meetings), auto-generate text transcripts and share as AIFF or M4A

QR CODES
Scan QR codes. Links can be verified in advance and force use of secure browser

APP CONFIG
Apply app configurations for managed Open In, auth, copy/paste, printing, and more. Also add any combination of up to 40 custom configurations

COMPLIANCE
Insider Threat monitoring and alert system for DLP violations (screenshots, unauthorized sharing)

BACKUP
Set up automatic and manual encrypted content backups via SMB, WebDAV, SFTP, OneDrive©, or Blackberry©, Docs.

SEARCH
OCR and speech recognition allow content to be identified by audible words in audio/video or text ID in photos and documents. Search also encompasses notes and annotations.

EMM
Configure and manage with corporate Enterprise Mobility Management platform. (ex. Ivanti/MobileIron, BlackBerry, InTune, VMware, Citrix, MaaS360, or AppTec)

DATA PROTECTION
All captured Content remains in containerized storage under complete control. Content is never processed or stored on Inkscreen servers and data collection is limited to what is necessary for license management and support

- **Data Controls**: Enable viewing, filtering, sorting, and searching of documents. Control the storing, accessing, sharing, transferring, and archiving. Support e-signature annotations. All of these functions are handled within policy.

Governance Functions:

- **Policy Control**: Enforces policies for secure content capture, storage, access, transfers, and archives.
- **Compliance**: Provide a system to monitor, log, alert, and report on suspected data loss violations (such as screenshots and unauthorized sharing).

KEEP YOUR EYE ON THE CAMERA

Pictures, be they crudely drawn on a cave wall or digitally stored in a smart phone, convey vast amounts of information. Today's technology make it so easy to take pictures. The camera's phone vastly improves productivity. Many applications leverage the camera for a wide range of purposes. It would be unproductive to prevent the use of the camera. Research indicates 87% of businesses allow their employees to access work resources from personal mobile devices. Companies have learned that people skirt the prohibitions placed on them. Phone cameras have many positives, but they also have vulnerabilities which must be mitigated.

The risks associated with a smartphone's camera and supporting applications need to be directly addressed within a comprehensive security policy. Optimum mobile security starts with mobile device management (MDM). However, MDM is only one component. Organizations need to ensure they can isolate data using containers. Data containers makes it possible to separate business files from personal files. In this way business files are secure and handled according to corporate policies and industry regulations. Encryption ensures data confidentiality. Workflow is also a key component in protecting the data collected using mobile devices.

CAPTOR™ from Inkscreen

What is normally overlooked in the mobile device security equation is full control of captured data. CAPTOR™ from Inkscreen provides this critical capability. Critical and sensitive information is easily created with a mobile device and supporting applications. Protecting that information is difficult. Employees crave the freedom of unrestricted use of their smartphones. CAPTOR allows a business to find the right balance between user satisfaction, productivity, business operations, and content protection.

The Inkscreen CAPTOR app combines the functionality of a professional camera app, document scanner, video recorder, and QR Code reader. It can be deployed and managed by many of the leading Enterprise Mobile Management (EMM). The solution enables the secure capture and management of sensitive business-related content—scanned documents and photos, and video recordings. Mobile users can still store and share files, but all of this is conducted in compliance with the organization's security policy. The solution leverages IT policies, metadata and watermarking to identify, track and manage captured content. With CAPTOR the enterprise gains digital rights protection. The user also gains privacy protection. Personal files are not accessible by the business and will not be removed should the company need to wipe corporate information from the device.

CAPTOR from Inkscreen is the security mobile application that allows enterprises to keep a close eye on mobile device camera activities. It provides visibility and control, enabling employees to use the mobile devices they are most comfortable with. By empowering the business use of OCR, photos, and video employees can be more productive. Risks of misuse, data loss, and compliance violations are greatly reduced.

ABOUT INKSCREEN

Inkscreen was founded in 2012 to provide enterprise-ready mobile applications to manage and control sensitive content captured on mobile devices. The company founders have extensive backgrounds in enterprise mobility, Fortune 500 IT consulting and ERP software.

For more information, please visit: **http://www.inkscreen.com**.