Privacy Challenges for Smart-Cities

The Challenge of IoT “Camera Uberveilance”

http://bit.ly/CameraPrivacy2019

Who am I?

- IEEE Volunteer (Electronic & ICT Engineer)
  - Board Member of IEEE Consumer Electronics Society *(6 years)*
  - Editor-in-Chief of IEEE Consumer Electronics Magazine *(2010-2016)*
  - IEEE Fellow in 2010 *(Contributions to Digital Camera Technology)*
  - IEEE Distinguished Lecturer, Conference Chair, Editor & Reviewer
- Day Job(s):
  - University Professor & Former Vice-Dean *(Research & Grad Studies)*
  - Active Researcher *(currently 10 PhD & 3 PostDoctoral researchers)*
  - Entrepreneur, Inventor & Technologist;
  - Industry Consultant
- Contact Information
  - E-Mail: dr.peter.Corcoran@ieee.org
  - Twitter: @pcor LinkedIn:
  - Google Scholar: https://scholar.google.com/citations?hl=en&user=J6YWBB4AAAAJ

What is in this Talk?

1) A Privacy Responsibility Framework for IoT (form WF_IoT 2016)
2) Cameras are Everywhere in Smart-Cities
   cheap camera tech + G5 + cloud infrastructure = Uberveillance
3) What's inside a Camera?
   Today's cameras and some ideas on how they can & will change …
4) Two Approaches to Protecting Privacy
   The Anonymization Approach - stop sending images to the cloud!
   The De-Identification Approach – authenticate, track and de-identify 'registered' citizens
5) Thoughts & Take-Aways

Corcoran PM. A Privacy Framework for the Internet of Things.
In: 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) 2016 Dec 12 (pp. 13-18). IEEE.

1. A Privacy Responsibility Frame-work for the Internet-of-Things

Concluding thoughts & reflections on building a Privacy framework for IoT …

Some Key principles for a Privacy Framework #1

- ***Privacy at the Edge:*** privacy issues should be addressed at the data source.
    - For IoT this implies that privacy sensitive data should be protected at the point of data acquisition/creation.
    - One example previously detailed, is to obfuscate sensitive biometric data (e.g. faces) in images at the point of acquisition.
    - Other data may need to be preserved in the original form in which case it could be encrypted at source.
- ***Privacy-aware Devices:*** modern personal devices are prolific data and content sources – generate many GB data per month.
    - Almost all of this data can be associated with some class of privacy risk and some risks can extend beyond the privacy of the user of the device.

Some Key principles for a Privacy Framework #2

- ***Industry Engagement with Privacy:***
  - There is a strong mandate for an industry-wide set of guidelines for device manufacturers and sub-system suppliers.
  - As IoT devices begin to proliferate online & network service providers should also engage with such efforts.
- ***Broader Co-operation between Industry and Regulators:***
  - There is a need for increased co-operation between the manufacturers of devices, components, networking equipment, online service providers, standards bodies, infrastructure owners and public bodies & regulators to strongly encourage more privacy-transparent policies and architectural standards.
  - A privacy-friendly digital ecosystem *should be everybody's business*. And in everyone's interest in the long run!

Point #1 from Today's Presentation

In 2016 no one really cared too much about privacy on mobile devices! *In 2019 your corporate reputation depends on it!*

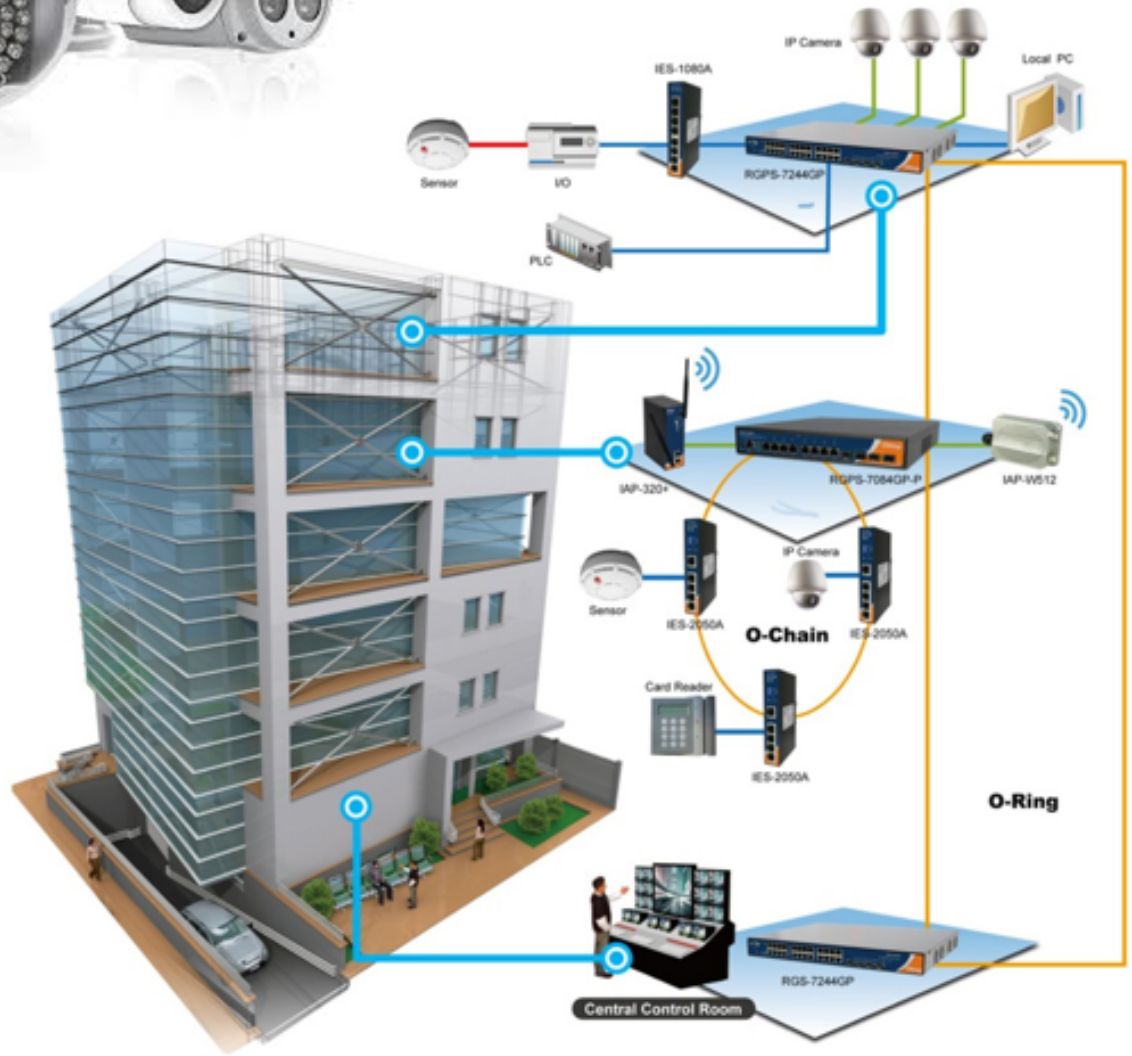
http://bit.ly/CameraPrivacy2019

Cameras are Everywhere in the Smart-City

http://bit.ly/CameraPrivacy2019

On the Streets

In the Buildings



http://bit.ly/CameraPrivacy2019

By the Roadways

In the Vehicles themselves …

Driver Monitoring Systems required in EU from 2021!

http://bit.ly/CameraPrivacy2019

At Airports …

On the people themselves …

http://bit.ly/CameraPrivacy2019

Even in your Home

http://bit.ly/CameraPrivacy2019

Point #2 from Today's Presentation

Cameras are everywhere and with IoT – ***all that data will end up in the Cloud!***

http://bit.ly/CameraPrivacy2019

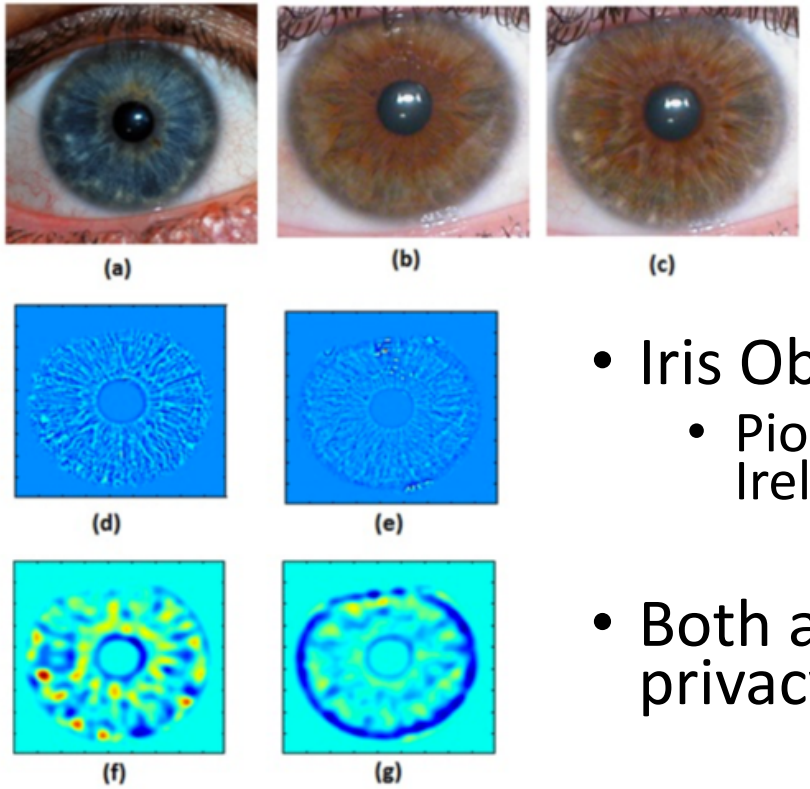
But then what happens to Privacy?

When you are THE World's DATA HUB …

… You need the World's Biggest Data Center to store all that Cloud Data!

Fighting Back!

- Urban Camoflague
  - Pioneered by New-Yorkers!



- Iris Obfuscation
  - Pioneered in by researchers in Galway, Ireland & Bucharest, Romania

- Both are reactions to increasing privacy challenges!

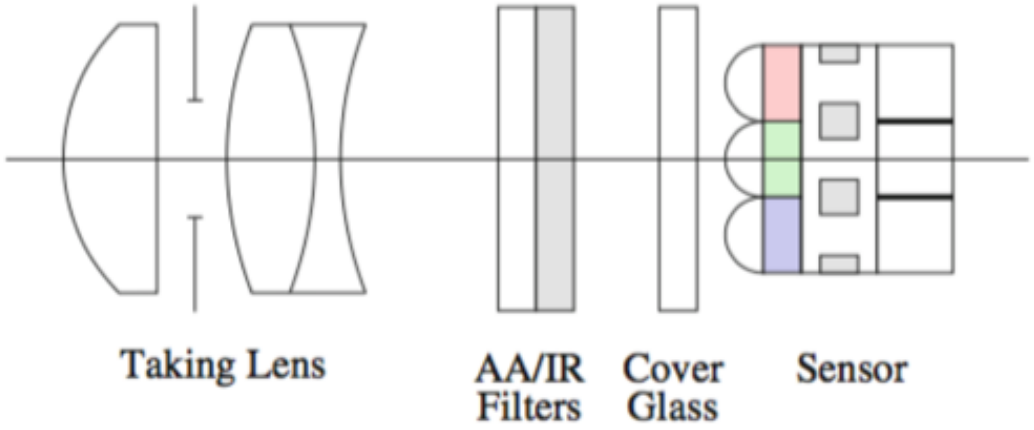
2. What is inside a Camera?

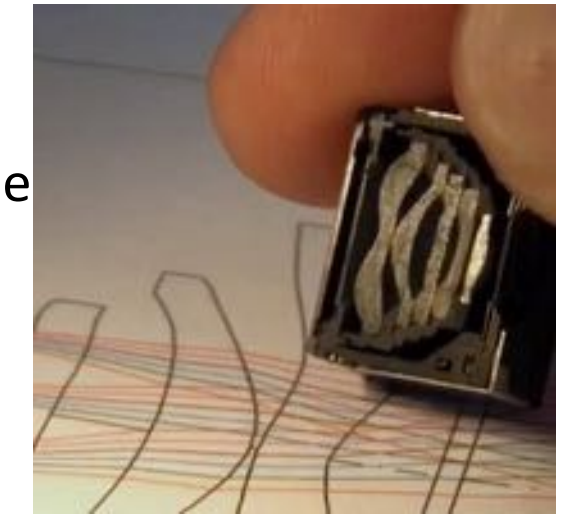
& Why are they everywhere in Smart-Cities?

Digital Camera Technologies #1

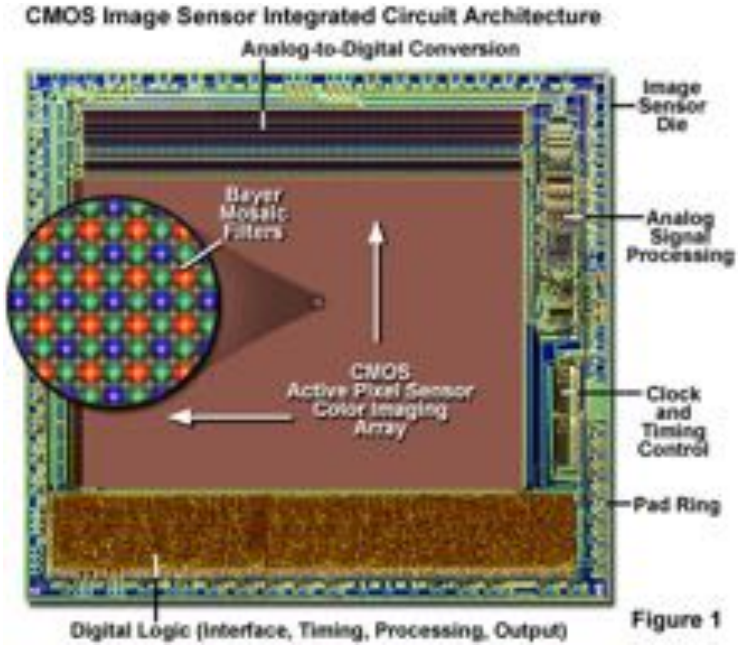
Basics – The Optical Image Path #1

- Multi-Element Lens
  - Typically at least 5-element
  - Telecentric (see reading #1)
  - Small Point-Spread Function (PSF)
- Anti-Aliasing Filter
  - Removes High-Frequency (Spatial) Artifacts
- Infrared Cutoff Filter
  - Silicon is sensitive to NIR
  - NIR focus is different to Visible
- Sensor
  - Bayer Color Filter Array (CFA)
  - Back-Illuminated



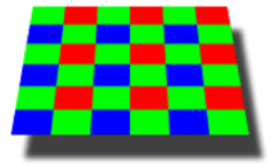


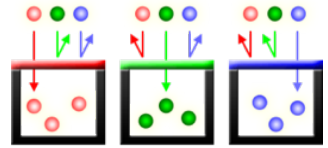
http://bit.ly/CameraPrivacy2019



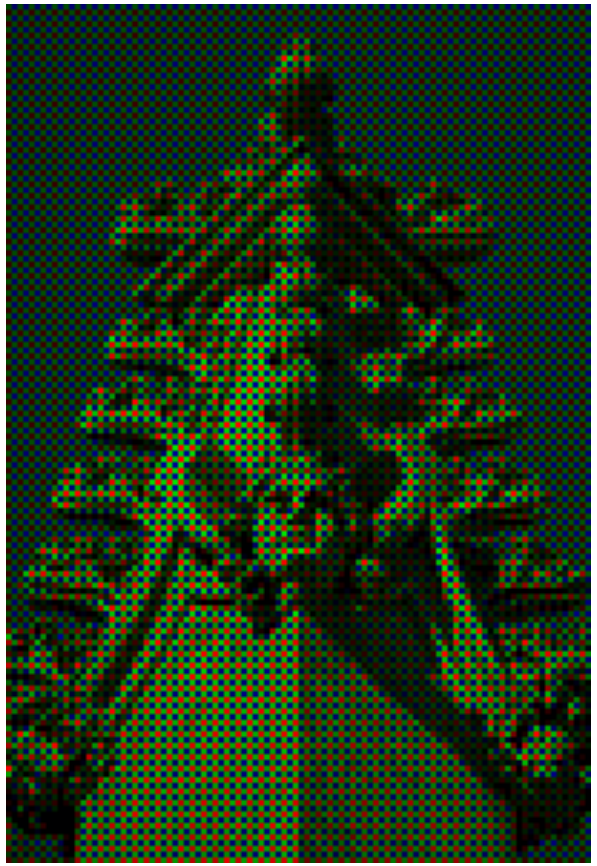
Digital Camera Sensors #3

Bayer Image





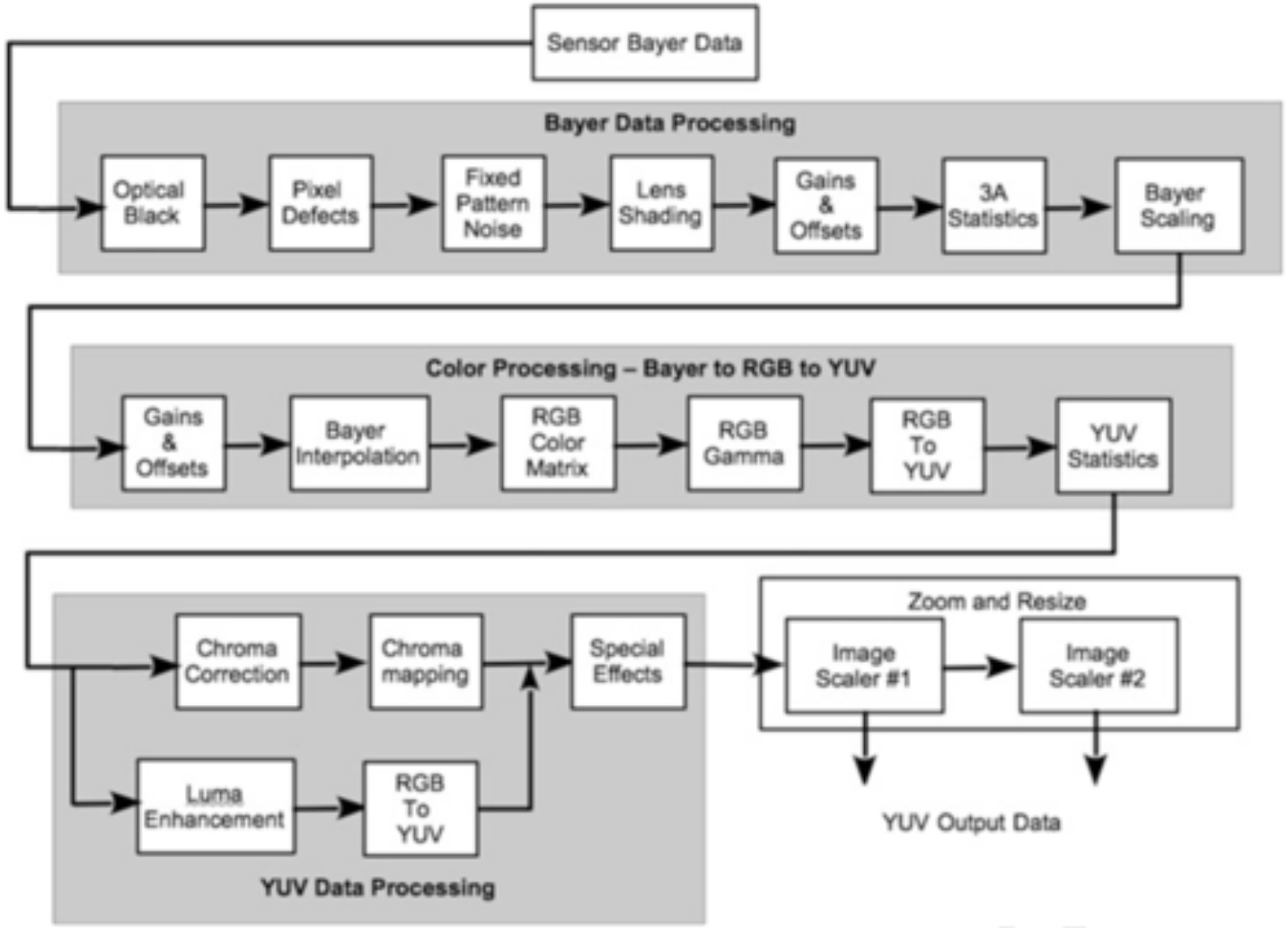
- A Bayer array consists of alternating rows of red-green and green-blue filters.
- Notice how the Bayer array contains twice as many green as red or blue sensors.
- Each primary color does not receive an equal fraction of the total area because the human eye is more sensitive to green light than both red and blue light.
- Redundancy with green pixels produces an image which appears less noisy and has finer detail than could be accomplished if each color were treated equally.
  - Noise in the green channel is less than for the other two primary colors simply because there are twice as many pixels.
- Bayer's technique is > 30 years old – clearly a robust engineering approximation!



Digital Camera Technologies #16

Basics – The image Processing Pipeline #1

- To fully understand the complexity of what happens in a modern digital camera, we need to illustrate the concept of the image processing pipeline (IPP) – the sequence of digital manipulations of the original image data to get to the image that you see on the main camera screen.



Digital Image & Compression Basics #6

compression - JPEG #1

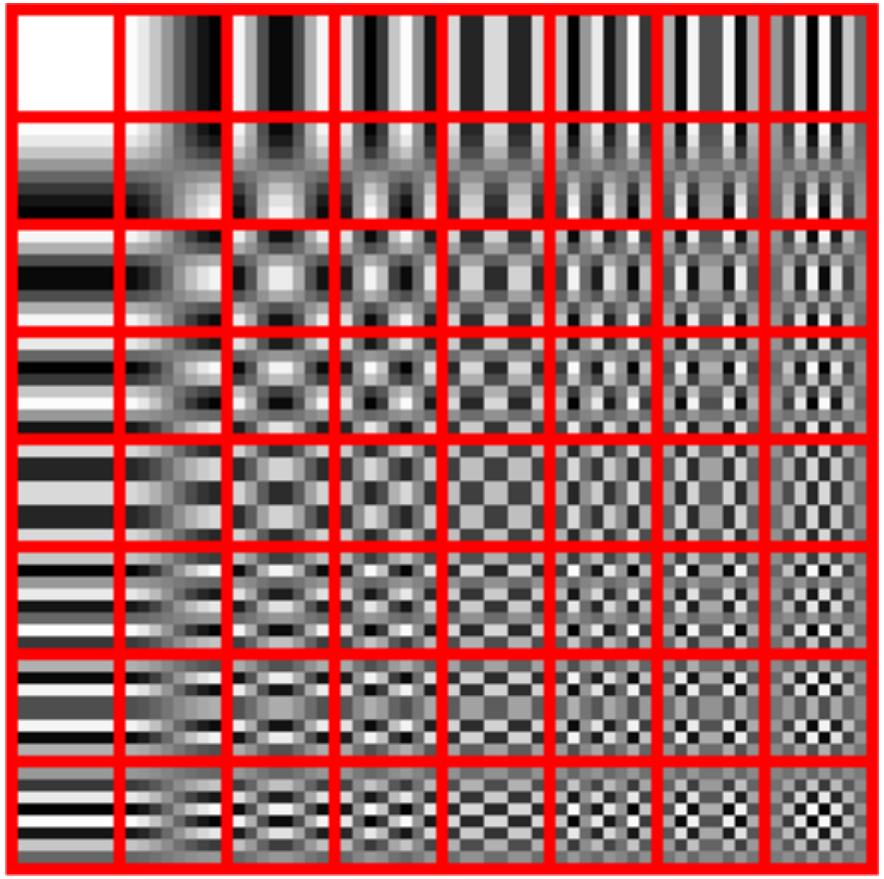
- **JPEG** is a commonly used method of lossy compression for digital images, particularly for those images produced by digital photography.
- The degree of compression can be adjusted, allowing a selectable tradeoff between storage size and image quality.
  - JPEG typically achieves 10:1 compression with little perceptible loss in image quality.
- **JPEG/Exif** is the most common image format used by digital cameras and other photographic image capture devices; along with **JPEG/JFIF**, it is the most common format for storing and transmitting photographic images on the World Wide Web.
- The term "JPEG" is an acronym for the **Joint Photographic Experts Group,** which created the standard.
- As the typical use of JPEG is a lossy compression method, which somewhat reduces the image fidelity, it should not be used in scenarios where the exact reproduction of the data is required (such as some scientific and medical imaging applications and certain technical image processing work).

A photo of a cat with the compression rate decreasing, and hence quality increasing, from left to right.

Digital Image & Compression Basics

compression - JPEG #3

- **JPEG encoding example:** Although a JPEG file can be encoded in various ways, most commonly it is done with JFIF encoding. The encoding process consists of several steps:
  - **Color Space Transformation:** the representation of the colors in the image is converted from RGB to Y'CBCR. (This step is sometimes skipped.)
  - **Chroma Downsampling:** the resolution of the chroma data is reduced, usually by a factor of 2 or 3. This reflects the fact that the eye is less sensitive to fine color details than to fine brightness details.
  - **Block Splitting & DCT:** The image is split into blocks of 8×8 pixels, and on each block, each of the Y, CB, and CR data undergo a discrete cosine transform (**DCT**). A DCT is similar to a Fourier transform in the sense that it produces a form of **spatial frequency spectrum**.
  - **Quantization:** the amplitudes of frequency components are quantized - human vision system (HVS) is more sensitive to small variations in color or brightness over large areas than to high-frequency (edge) variations. Thus, the magnitudes of high-frequency components are stored with lower accuracy than low-frequency components.
  - The quality setting of the encoder affects to what extent the resolution of each frequency component is reduced. If a very low quality setting is used, the high-frequency components may be discarded altogether.
  - **Entropy Encoding:** The resulting data for all 8×8 blocks is further compressed with a lossless algorithm, a form of **Huffman encoding**.
- The decoding process reverses these steps, except the quantization because it is irreversible. Also, modern devices with larger image sensors may use 16x16 or larger DCT blocks.
  - A detailed example is given at: https://en.wikipedia.org/wiki/JPEG



The DCT transforms an 8×8 block of input values to a linear combination of these 64 patterns. The patterns are referred to as the 2D **DCT basis functions**, and the output values are **transform coefficients**. The horizontal index is **u** and the vertical index is **v**.

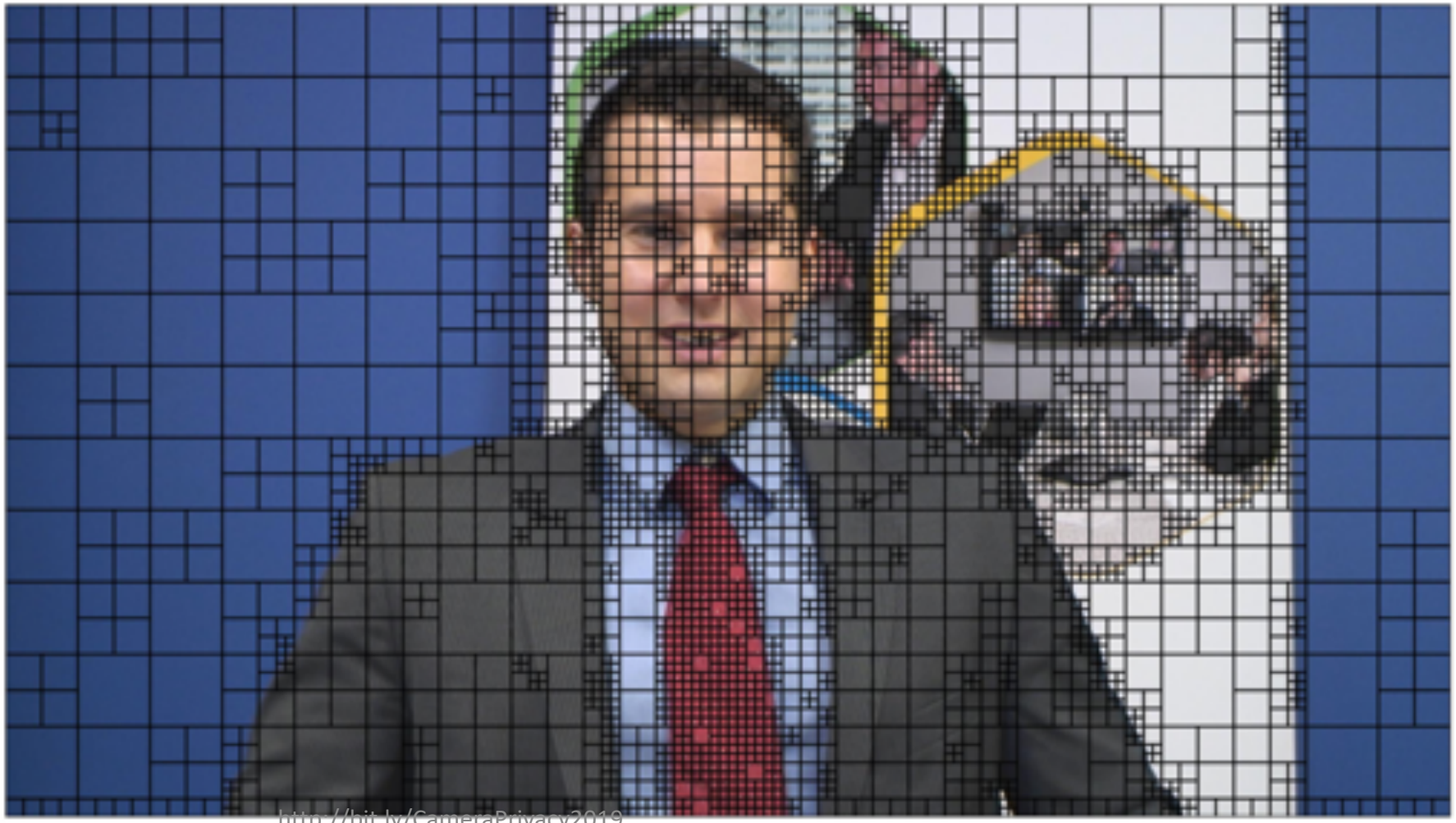
Digital Video Basics #10

Workings of HEVC #5

AVC used mainly a 4×4 transform and on occasion an 8×8 transform, HEVC has several transform sizes: 32×32, 16×16, 8×8 and 4×4.

From a matematical point of view, bigger TUs are able to encode better stationary signals while smaller TUs are better in encoding smaller "impulsive" signals. The transforms are based on DCT

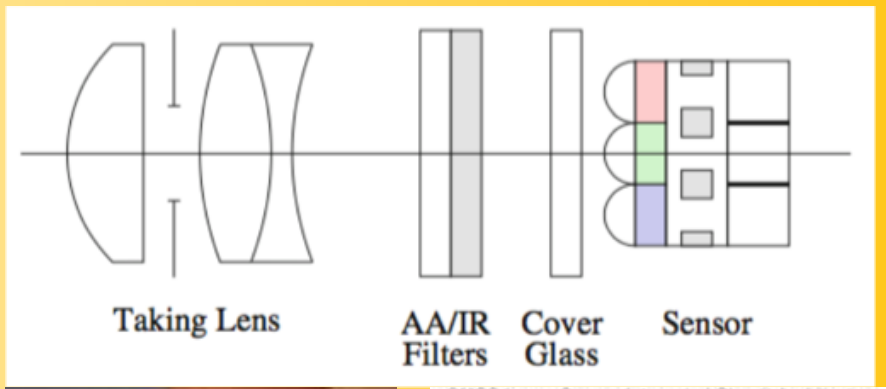
The **adaptive nature** of CBT, CU and TU partitions plus the **higher accuracy** plus the **larger transform size** are among the most important features of HEVC and the reason of the performance improvement compared to AVC.

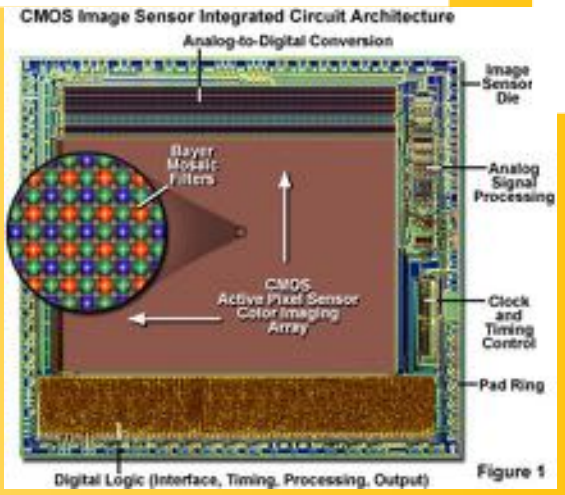


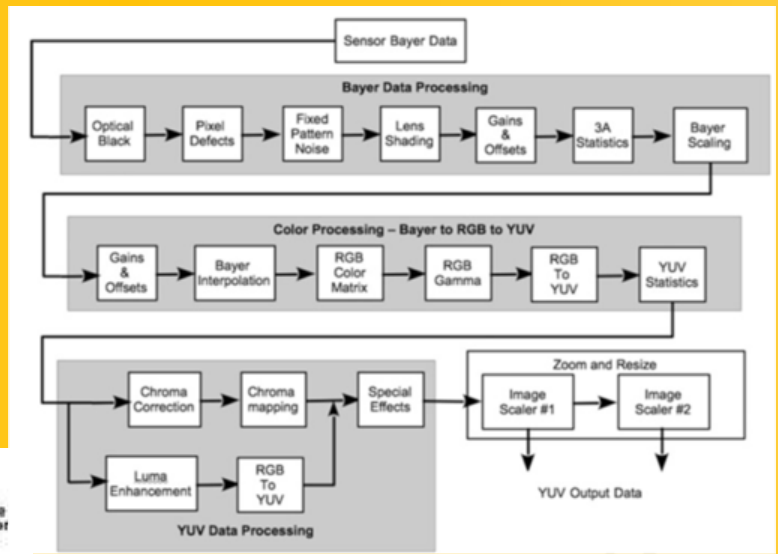
http://bit.ly/CameraPrivacy2019

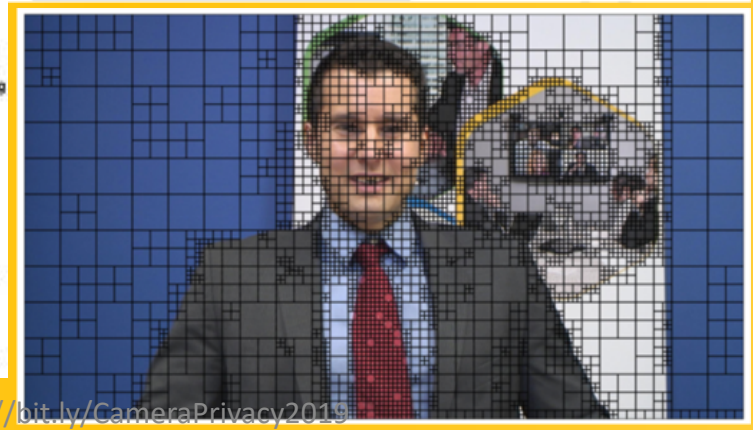
Point #3 from Today's Presentation

Camera Tech is incredibly sophisticated, but today it is a very *low-cost sensing commodity!*





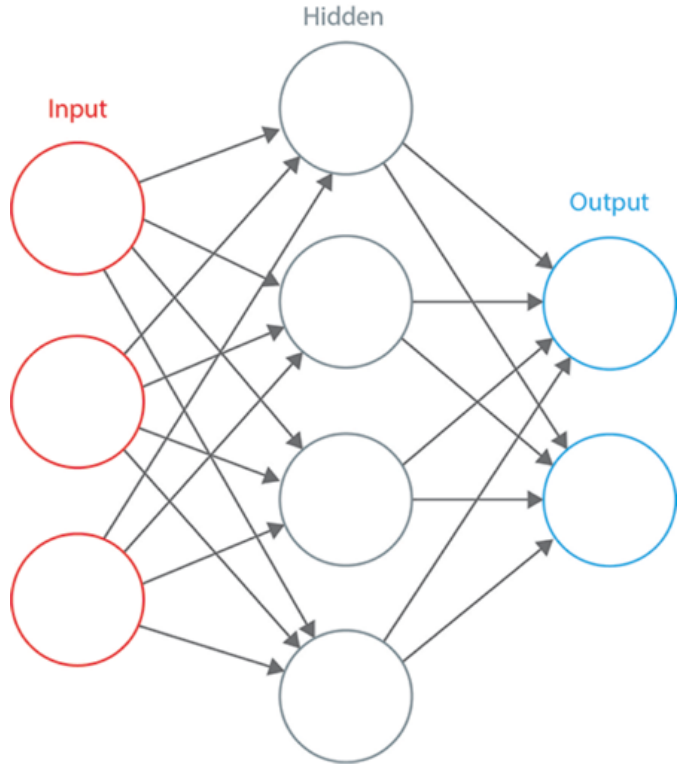


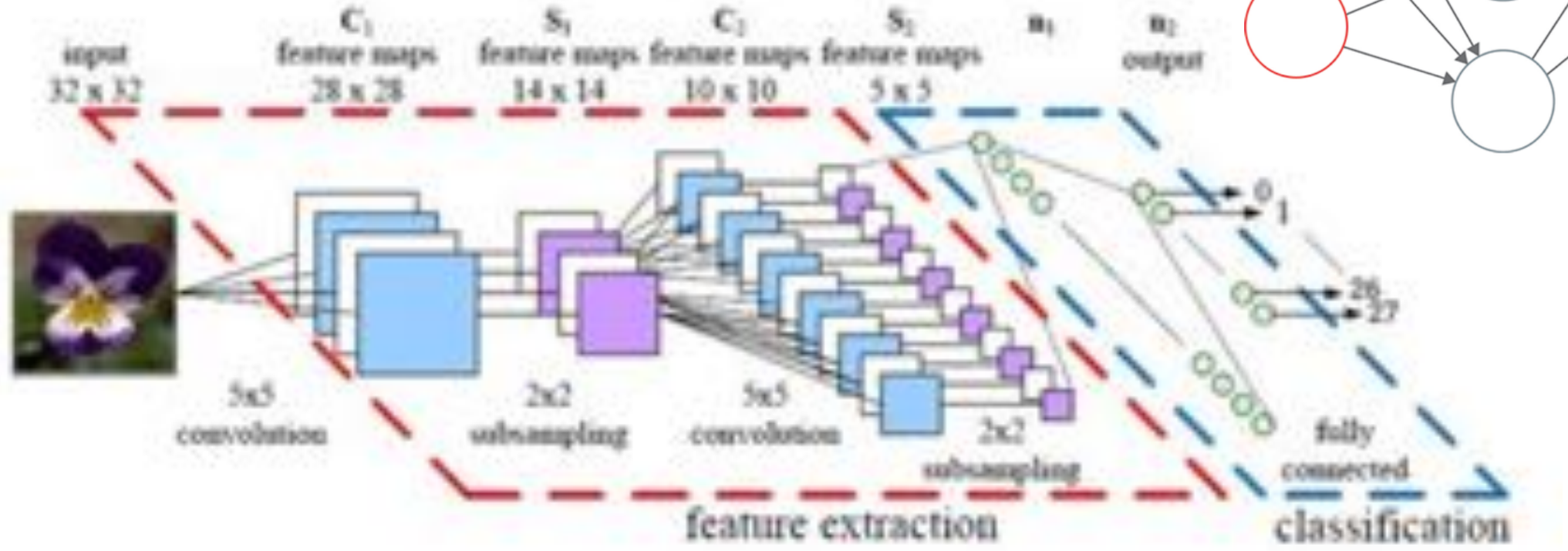


<$1

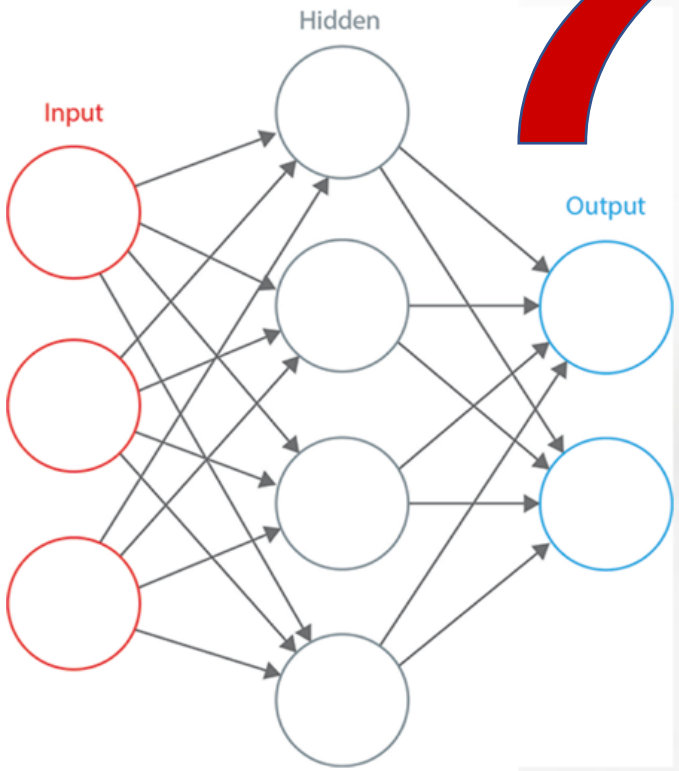
2.1. The Next Generation of Cameras?

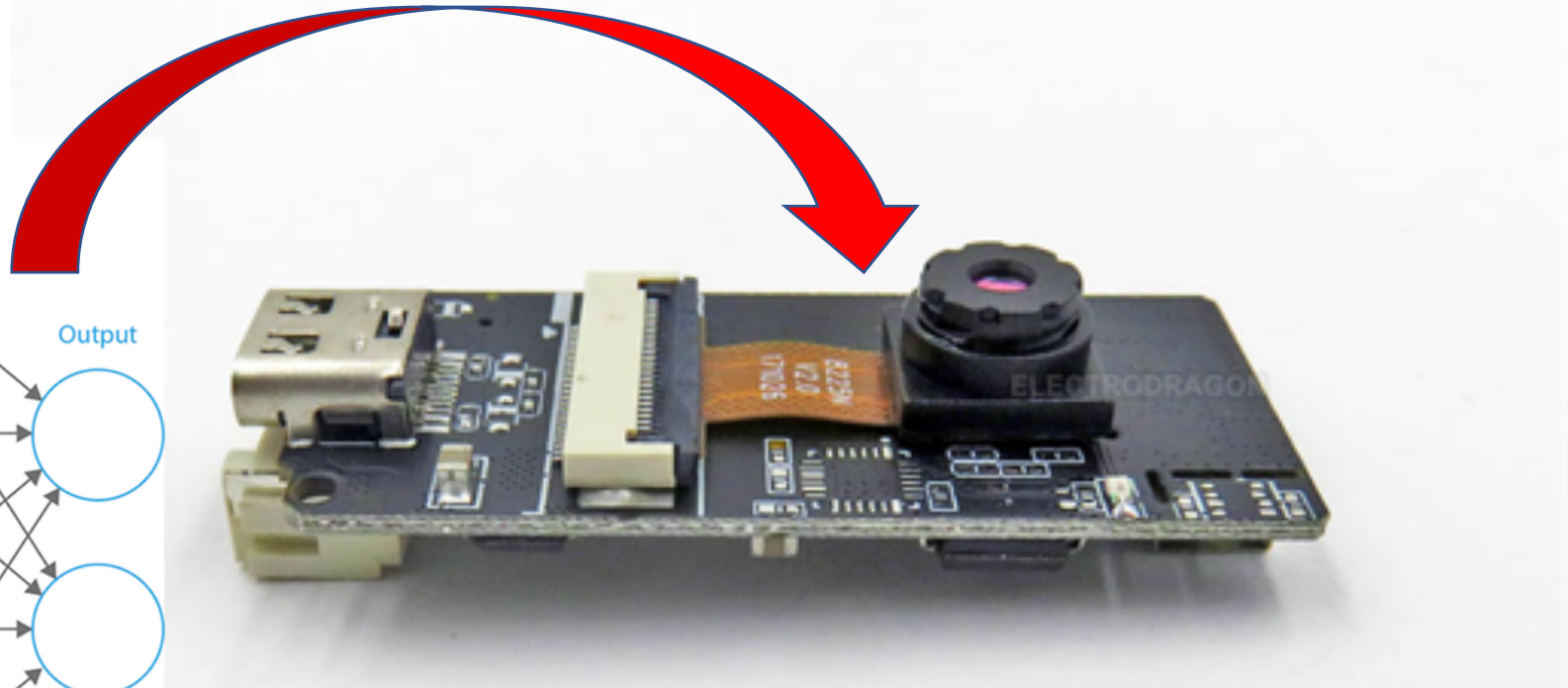
Convolutional Neural Networks (CNNs) ….





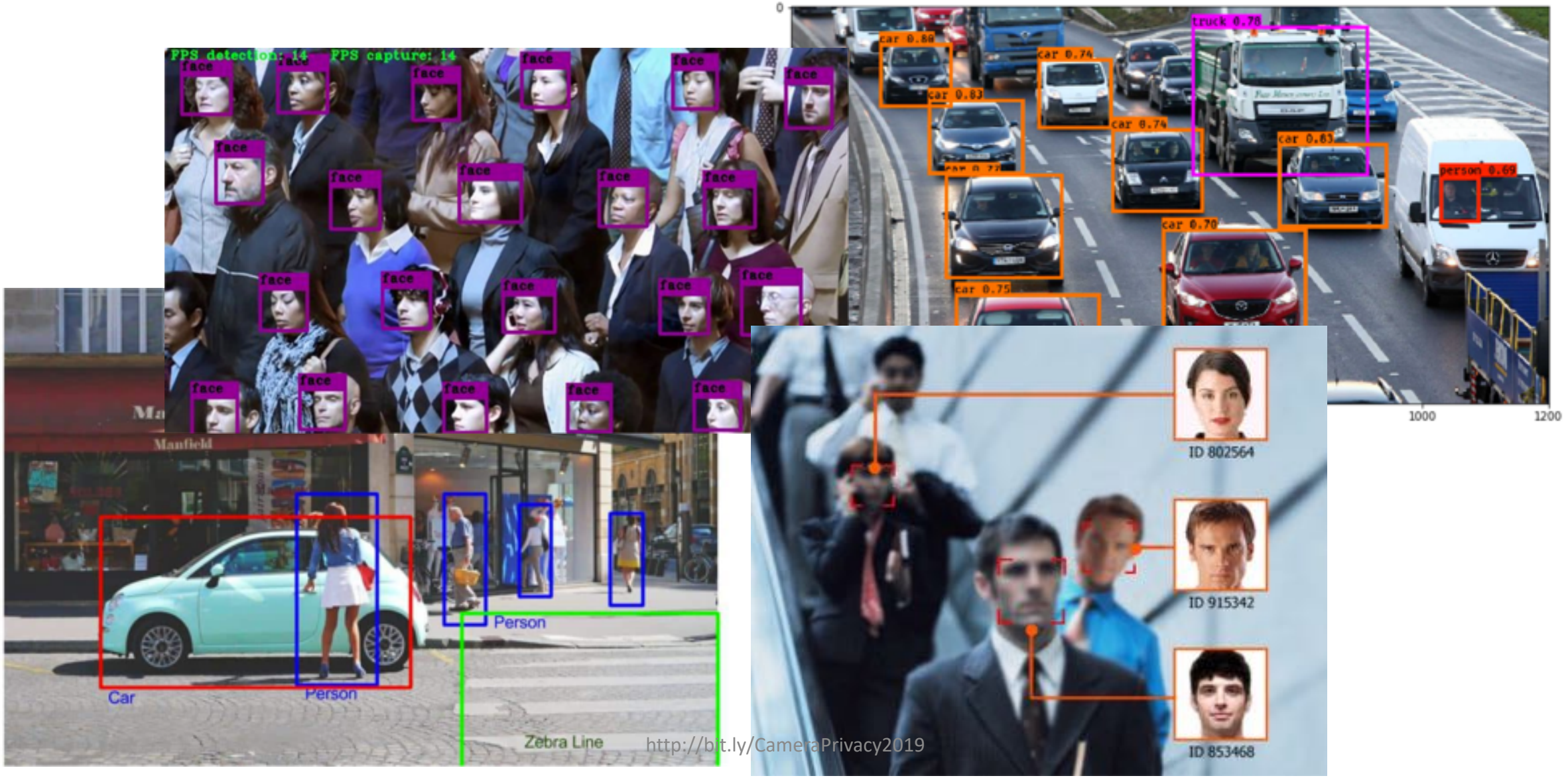
… embedded inside the camera!





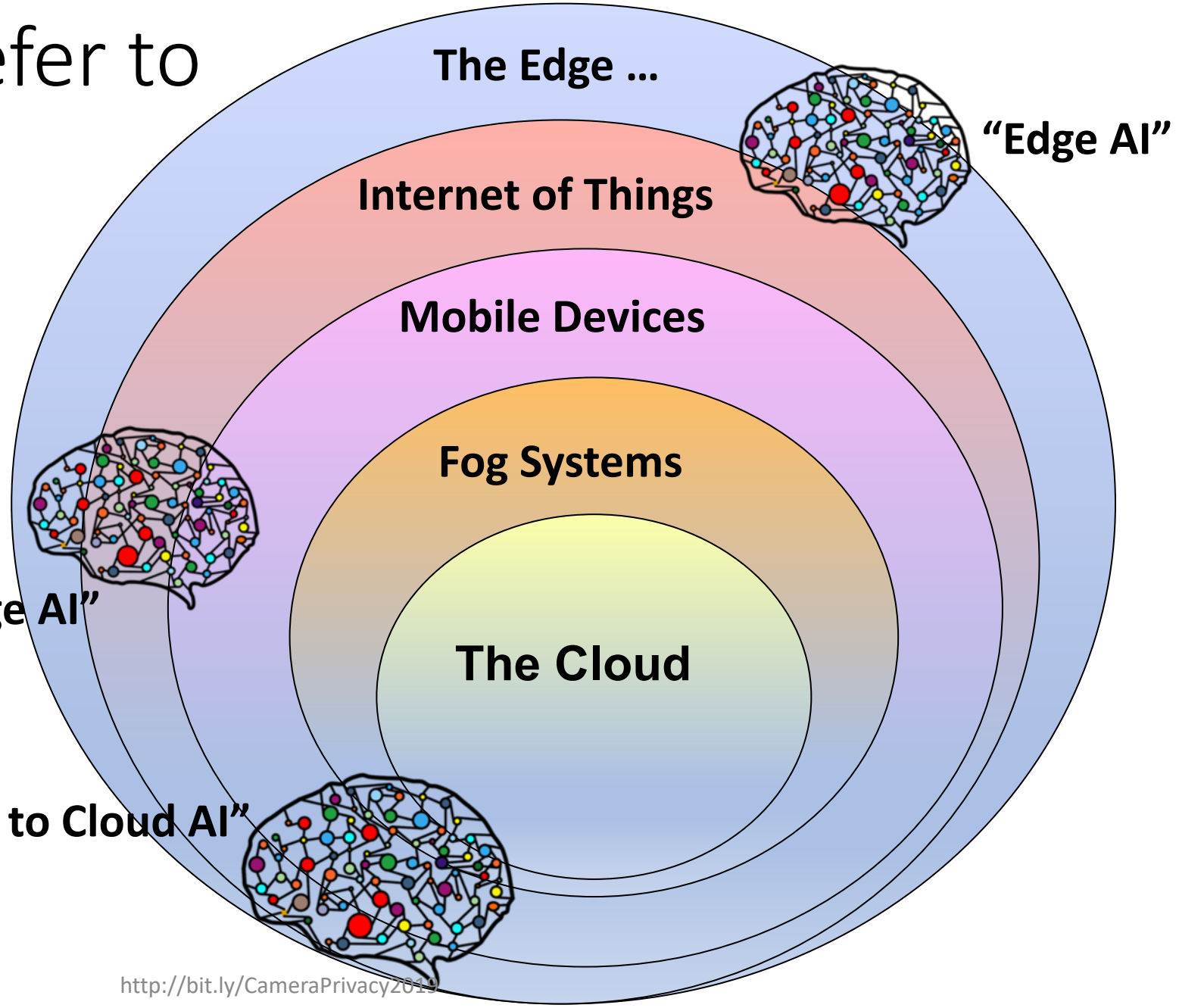
http://bit.ly/CameraPrivacy2019

To make a really “Smart” camera …

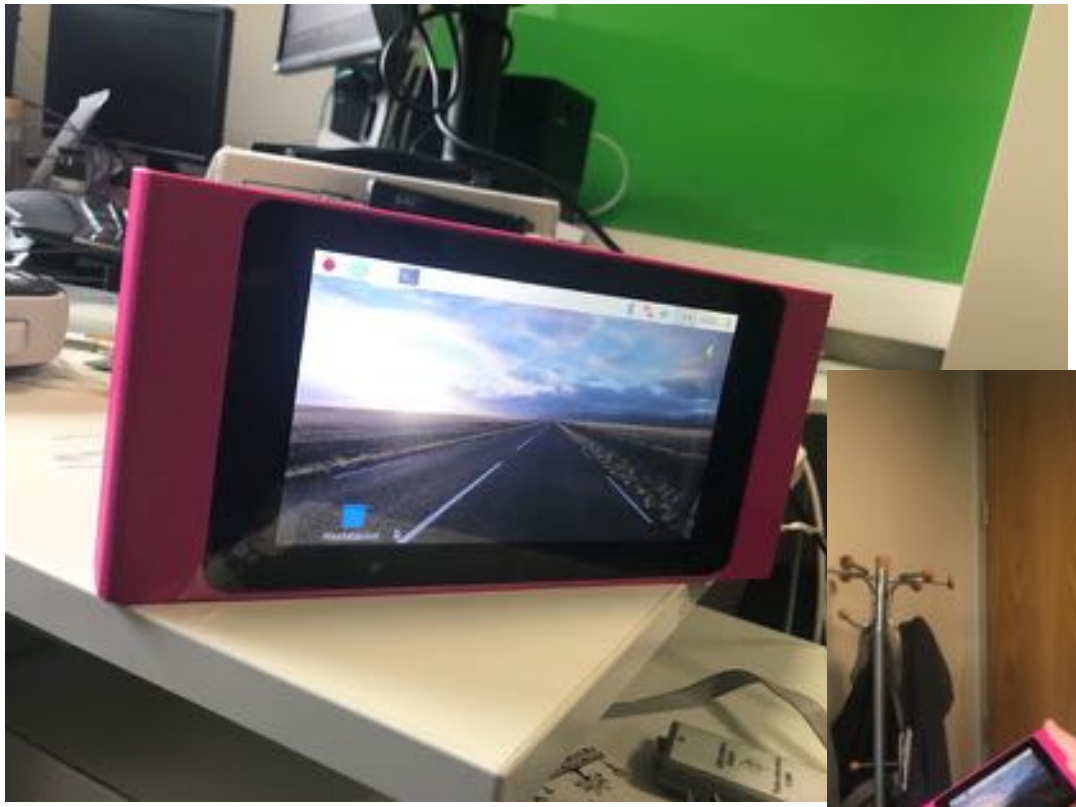


http://bit.ly/CameraPrivacy2019

This is what I refer to as “Edge AI” …



In fact we like Edge-AI so much we built a hand-held device to demonstrate what it is capable of …

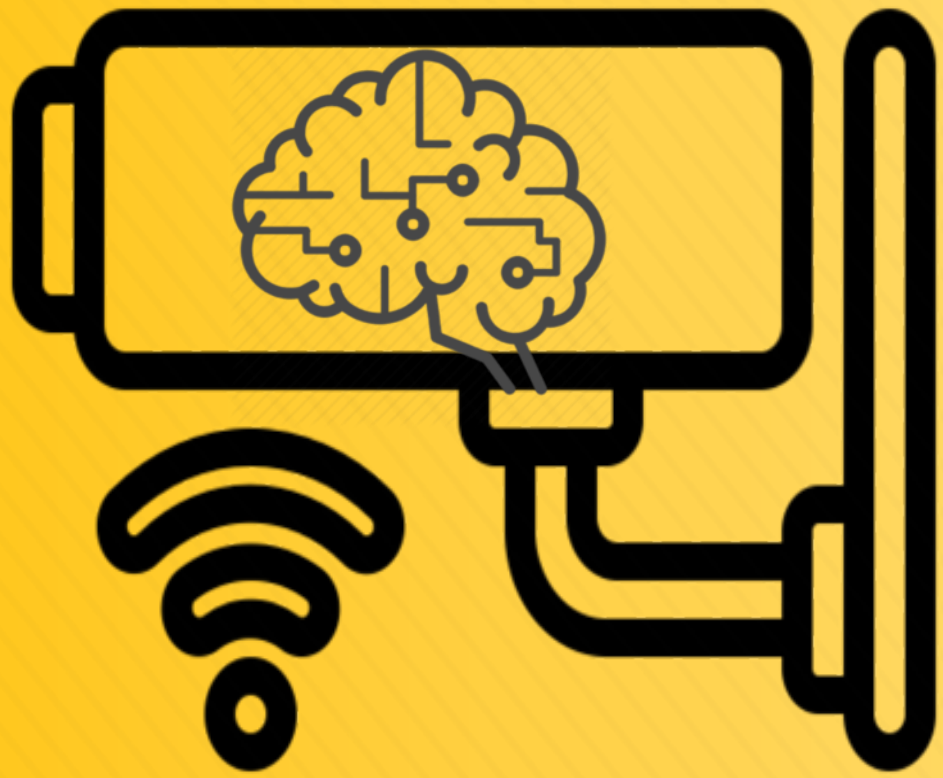


http://bit.ly/CameraPrivacy2019

Point #4 from Today's Presentation

Today's camera-technology is very sophisticated, but offers very ***low-cost sensing capabilities!***

The smart-camera can build in a lot of ***privacy protection at the Edge*** where sensing begins … is that enough?



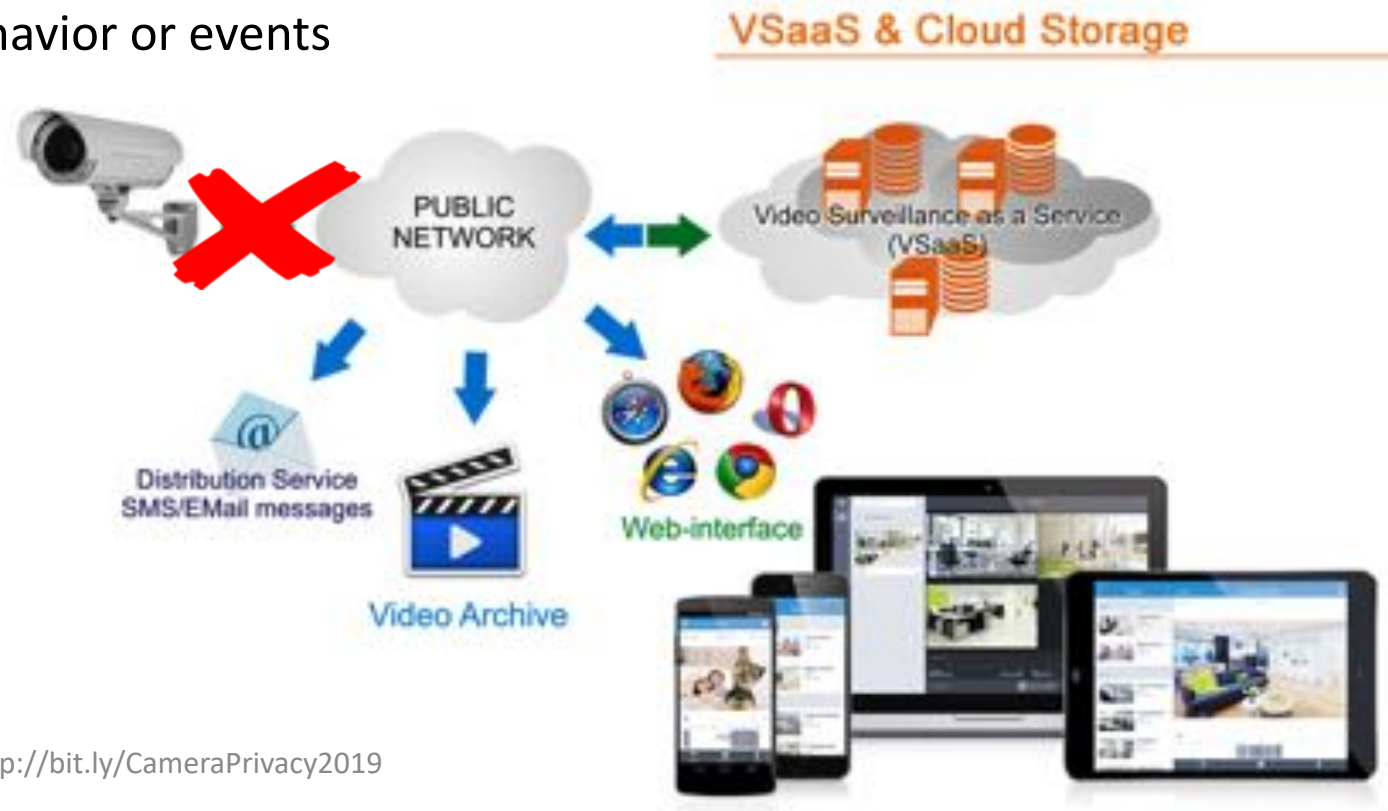
3. Protecting Privacy With Smart Cameras?

Two Approaches – Very, different ways to achieve digital privacy for residents in a Smart City!

First Approach - the *Anonymization Approach*

- Stop sending images & unnecessary data to the cloud!
  - In most smart-city use cases Cameras serve a specific purpose - some examples:
    - Count Traffic, Pedestrians, Commuters, Shoppers
    - Authenticate Access to a Building (Biometrics)
    - Monitor a street for unusual behavior or events

The camera does not need to send the raw image/video data to the network if it can apply Edge-AI to fulfil its purpose



http://bit.ly/CameraPrivacy2019

First Approach - the *Anonymization Approach #2*

- Thus ***limited data***, restricted to the ***sensory purpose of the camera*** is transmitted to support Smart-City operations
- Cameras are now cheap so we ***don't need to justify the cost by harvesting unnecessary data*** …

http://bit.ly/CameraPrivacy2019

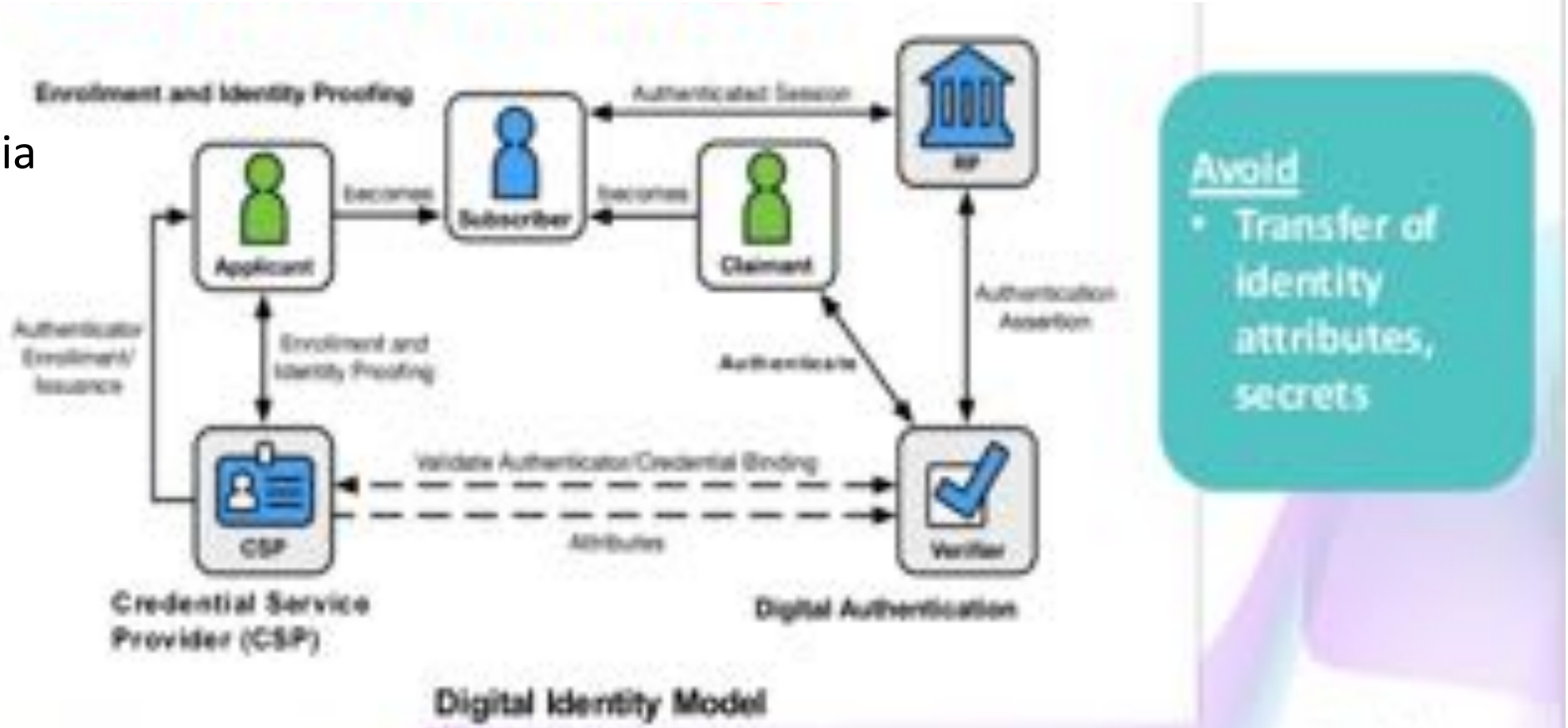
2nd Approach - the *De-Identification Approach (1)*

- Authenticate, track and de-identify ‘registered’ citizens
  - We can identify, authenticate & track people so lets use this to verify who is a bona-fide resident of the smart-city!

http://bit.ly/CameraPrivacy2019

2nd Approach - the *De-Identification Approach (2)*

- Residents can register for the ***De-ID*** service via a trusted 3rd party (TTP), or better a zero-knowledge proof (ZKP) service; this could be easily implemented with the aid of the residents smartphone;



2nd Approach - the *De-Identification Approach (3)*

- Now we can remove all data records pertaining to our verified resident from smart-city systems & storage;
- We can even initiate ***De-Identification*** at device (camera) level if a device can support a ***De-ID*** service!

2nd Approach - the *De-Identification Approach (4)*

- And to close the loop we should provide ***De-ID*** confirmation ***via a public ledger*** so that our residents can cross-check that their 'presence' has been removed from the data records of the smart-city;

Point #5 from Today's Presentation

Privacy starts at the *Edge* but that isn't enough in today's complex smart-city environments …

To genuinely ensure privacy we need to look at approaches that require *public accountability* – maybe this is a use-case where Blockchain Public Ledger technology makes sense?

??? Questions ???

Some articles to consider …

- Privacy, Smartphones & Internet of Things
  - P. Corcoran, “The Battle for Privacy In Your Pocket” [Notes from the Editor], IEEE Consumer Electronics Magazine. **2016** Jul;5(3):3-36.
  - P. Corcoran, “Privacy in the Age of the Smartphone”. IEEE Potentials. **2016** Sep;35(5):30-35.
  - P. Corcoran, “A privacy framework for the Internet of Things”, In Internet of Things (WF-IoT), **2016** IEEE 3rd World Forum on 2016 Dec 12 (pp. 13-18). IEEE.

- Biometrics & Personal Authentication
  - P. Corcoran, “Biometrics and consumer electronics: A brave new world or the road to dystopia?” [Soapbox]. IEEE Consumer Electronics Magazine. **2013** Apr;2(2):22-33.
  - P. Corcoran, C. Costache, “Biometric Technology and Smartphones: A consideration of the practicalities of a broad adoption of biometrics and the likely impacts”, IEEE Consumer Electronics Magazine, 5 (2), pp. 70–78, **2016**.
  - P. Corcoran, C. Costache, “Smartphones, Biometrics, and a Brave New World”, IEEE Technology and Society Magazine. **2016** Sep;35(3):59-66.

More articles to consider …

- Mobile Edge, IoT & Edge-AI
  - Corcoran P. Datta SK., Mobile-Edge Computing and Internet of Things for Consumers: Part II: Energy efficiency, connectivity, and economic development. IEEE Consumer Electronics Magazine. 2017 Jan;6(1):51-2..
  - Corcoran P, Datta SK. Mobile-edge computing and the Internet of Things for consumers: Extending cloud computing and services to the edge of the network. IEEE Consumer Electronics Magazine. 2016 Oct;5(4):73-4.
  - Corcoran P. The Internet of Things: why now, and what's next?. IEEE consumer electronics magazine. 2016 Jan;5(1):63-8.
- Deep Learning & Consumer Electronics use cases
  - Bazrafkan S, Corcoran PM. Pushing the AI envelope: merging deep networks to accelerate edge artificial intelligence in consumer electronics devices and systems. IEEE Consumer Electronics Magazine. 2018 Mar;7(2):55-61..
  - Lemley J, Bazrafkan S, Corcoran P. Deep Learning for Consumer Devices and Services: Pushing the limits for machine learning, artificial intelligence, and computer vision. IEEE Consumer Electronics Magazine. 2017 Apr;6(2):48-56.
  - Bazrafkan S, Javidnia H, Lemley J, Corcoran P. Depth from monocular images using a semi-parallel deep neural network (SPDNN) hybrid architecture. arXiv preprint arXiv:1703.03867. 2017 Mar 10.

And even more articles to consider …

- Deep Learning & Biometric use cases
  - Bazrafkan S, Thavalengal S, Corcoran P. An end to end deep neural network for iris segmentation in unconstrained scenarios. Neural Networks. 2018 Oct 1;106:79-95.
  - Varkarakis V, Bazrafkan S, Corcoran P. A Deep Learning Approach to Segmentation of Distorted Iris Regions in Head-Mounted Displays. In2018 IEEE Games, Entertainment, Media Conference (GEM) 2018 Aug 15 (pp. 1-9). IEEE..
  - Ungureanu AS, Thavalengal S, Cognard TE, Costache C, Corcoran P. Unconstrained palmprint as a smartphone biometric. IEEE Transactions on Consumer Electronics. 2017 Aug;63(3):334-42.
  - Bazrafkan S, Nedelcu T, Filipczuk P, Corcoran P. Deep learning for facial expression recognition: A step closer to a smartphone that knows your moods. In2017 IEEE International Conference on Consumer Electronics (ICCE) 2017 Jan 8 (pp. 217-220). IEEE.
  - Lemley J, Kar A, Drimbarean A, Corcoran P. Efficient CNN Implementation for Eye-Gaze Estimation on Low-Power/Low-Quality Consumer Imaging Systems. arXiv preprint arXiv:1806.10890. 2018 Jun 28.
  - Lemley J, Kar A, Drimbarean A, Corcoran P. Convolutional Neural Network Implementation for Eye-Gaze Estimation on Low-Quality Consumer Imaging Systems. IEEE Transactions on Consumer Electronics. 2019 Feb 15.