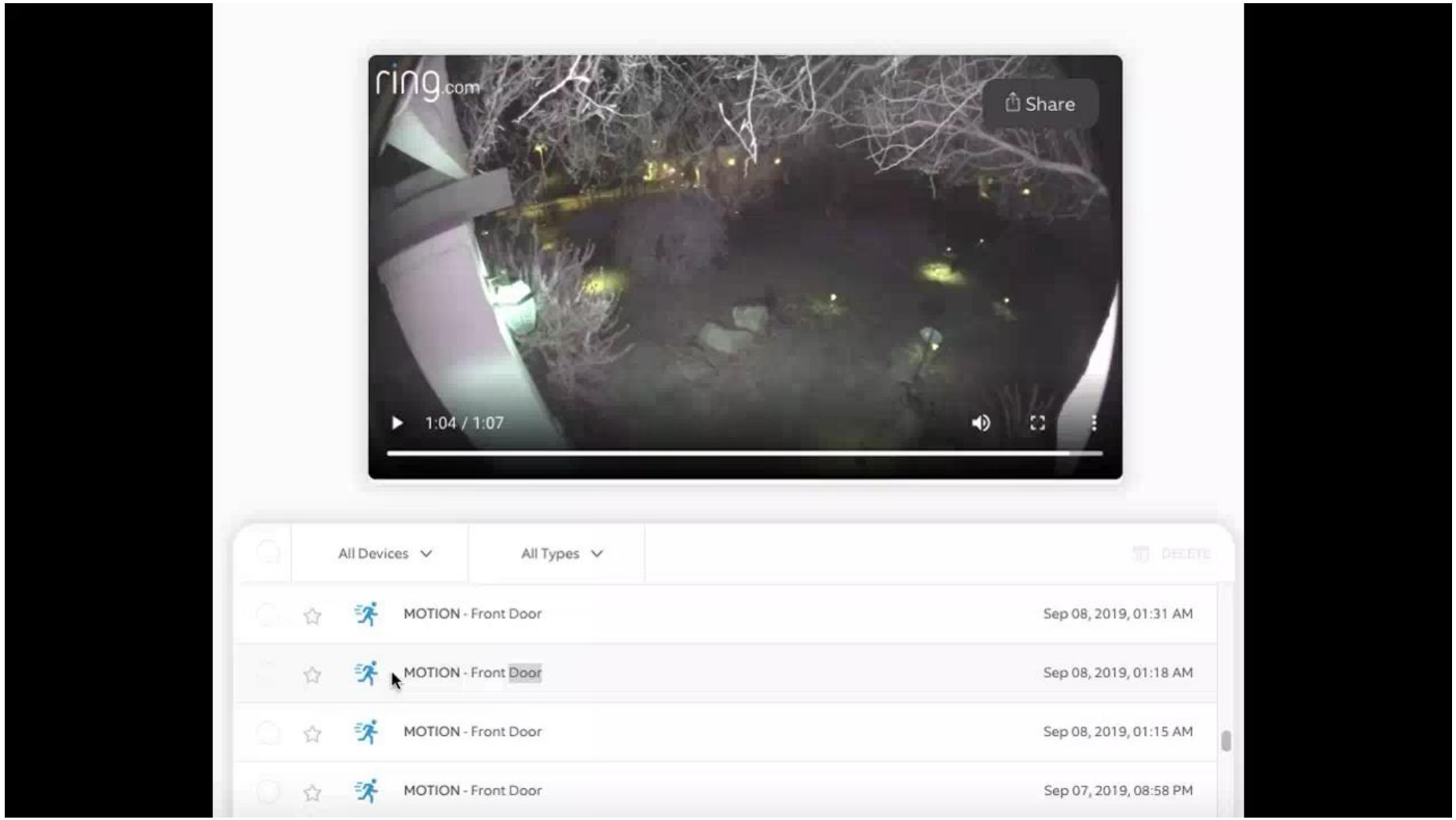
Managing Diverse Collections of Visual Data

VC, Security Applied Sciences Council
Chair, Public Safety Working Group

SURFARO LLC


Ring.com
ring


ring.com
Share
1:04 / 1:07
All Devices
All Types
DELETE
MOTION - Front Door
Sep 08, 2019, 01:31 AM
MOTION - Front Door
Sep 08, 2019, 01:18 AM
MOTION - Front Door
Sep 08, 2019, 01:15 AM
MOTION - Front Door
Sep 07, 2019, 08:58 PM

“Senator pushes Amazon for details about Ring “partnerships” with police”

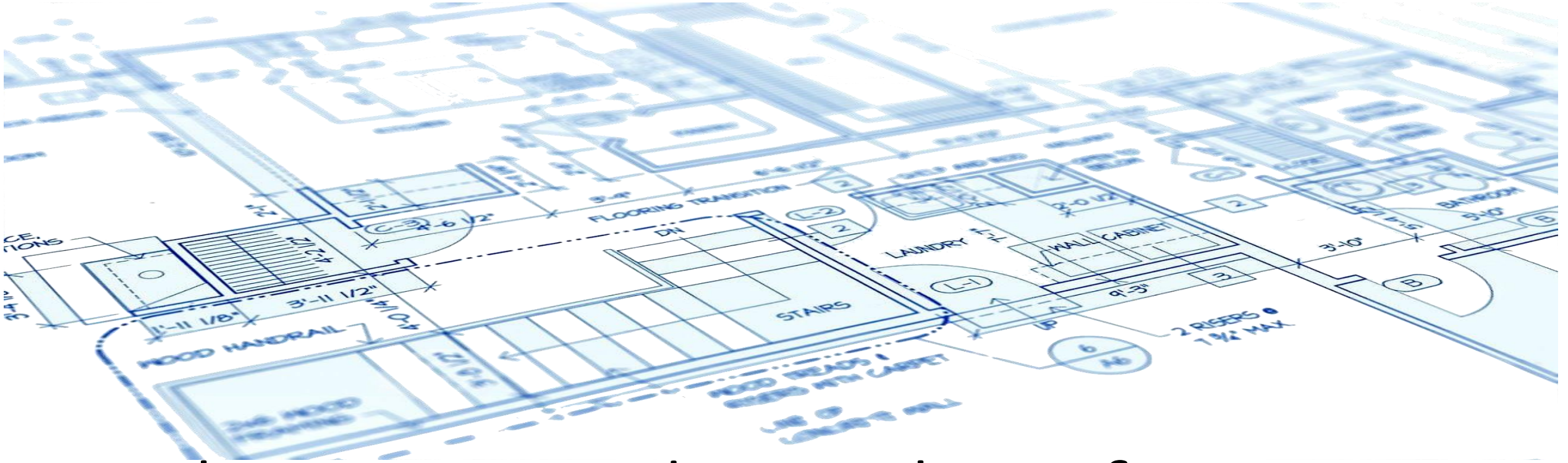
- Amazon's Ring line of video doorbells and home surveillance equipment is particularly popular with one key group: police. More than 400 law enforcement agencies around the country have partnered with Ring to use its apps and help market its security cameras to residents in the name of safer neighborhoods. "The nature of Ring's products and its partnerships with police departments raise serious privacy and civil liberties concerns," Markey said in a letter (PDF) addressed to Amazon CEO Jeff Bezos.
- "Although Amazon markets Ring as America’s ‘new neighborhood watch,’ the technology captures and stores video from millions of households and sweeps up footage of countless bystanders who may be unaware that they are being filmed," Markey said in a statement. "I am particularly alarmed to learn that Ring is pursuing facial-recognition technology with the potential to flag certain individuals as suspicious based on their biometric information."
- Ring said in late August it had 405 active agreements.

What are they worried about?

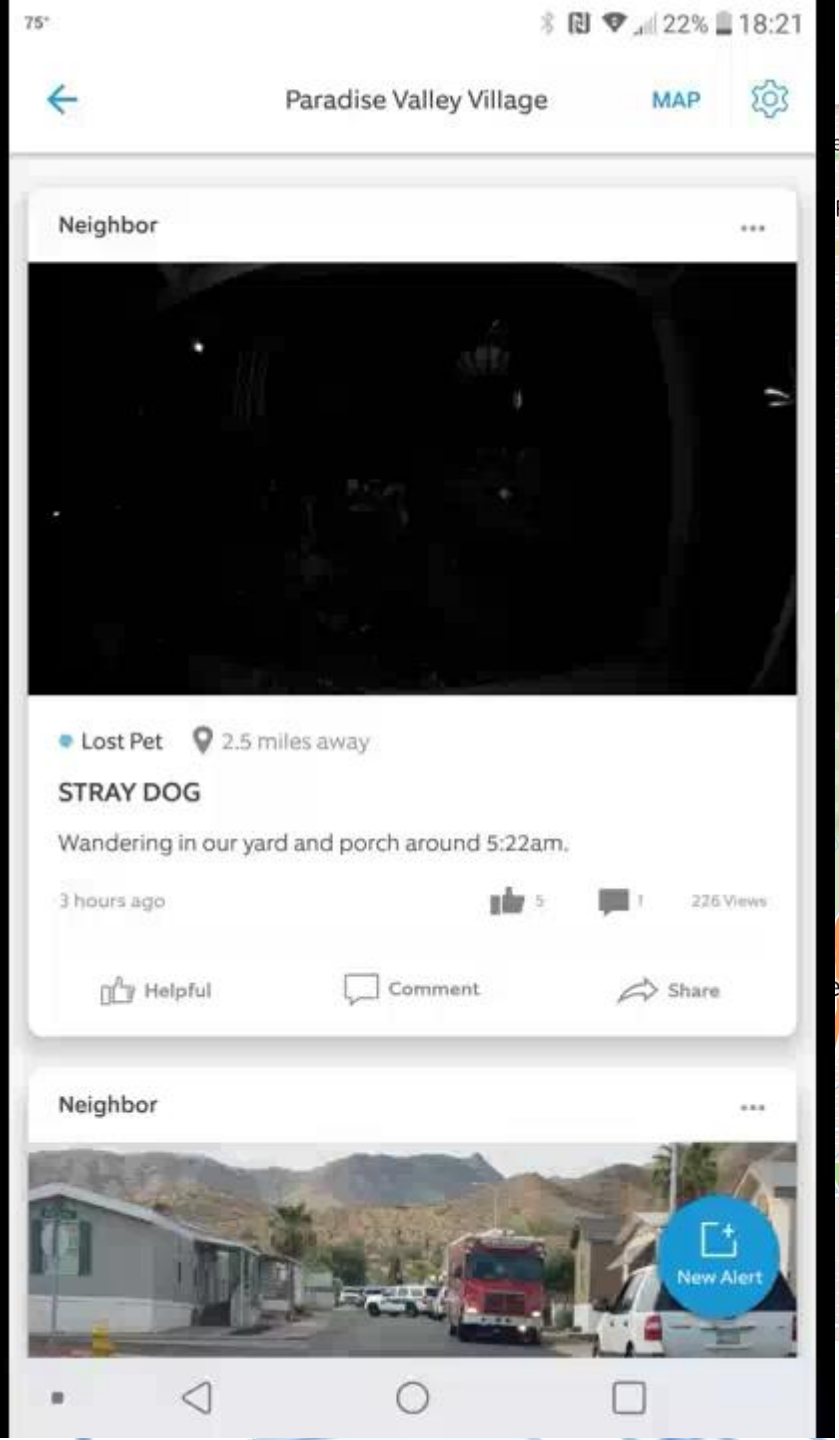
- Ring claims not to share lists of users or give maps pinpointing exact locations of cameras to police. In August, the company told Ars participating agencies "must go through the Ring team when making a video request to customers," adding, "Customers can choose to opt out or decline any request, and law enforcement agencies have no visibility into which customers have received a request and which have opted out or declined."
- Ring shared maps featuring active cameras with police in 2018.
- The company also gets access to 911 call data in some jurisdictions, which it uses to "curate" crime news for its Neighbors app. The app, while open to anyone, is optimized for Ring users, who can easily share footage from their doorbells through it. ~~Police can also use their companion portal to send out a localized blast to Neighbors users requesting footage as part of an investigation~~ *INCORRECT!*
- Late last year, the ACLU also flagged a patent application from Ring that would allow devices to ship with facial-recognition software, such as Amazon's Rekognition system. The patent would allow police or homeowners to flag certain faces as "suspicious."

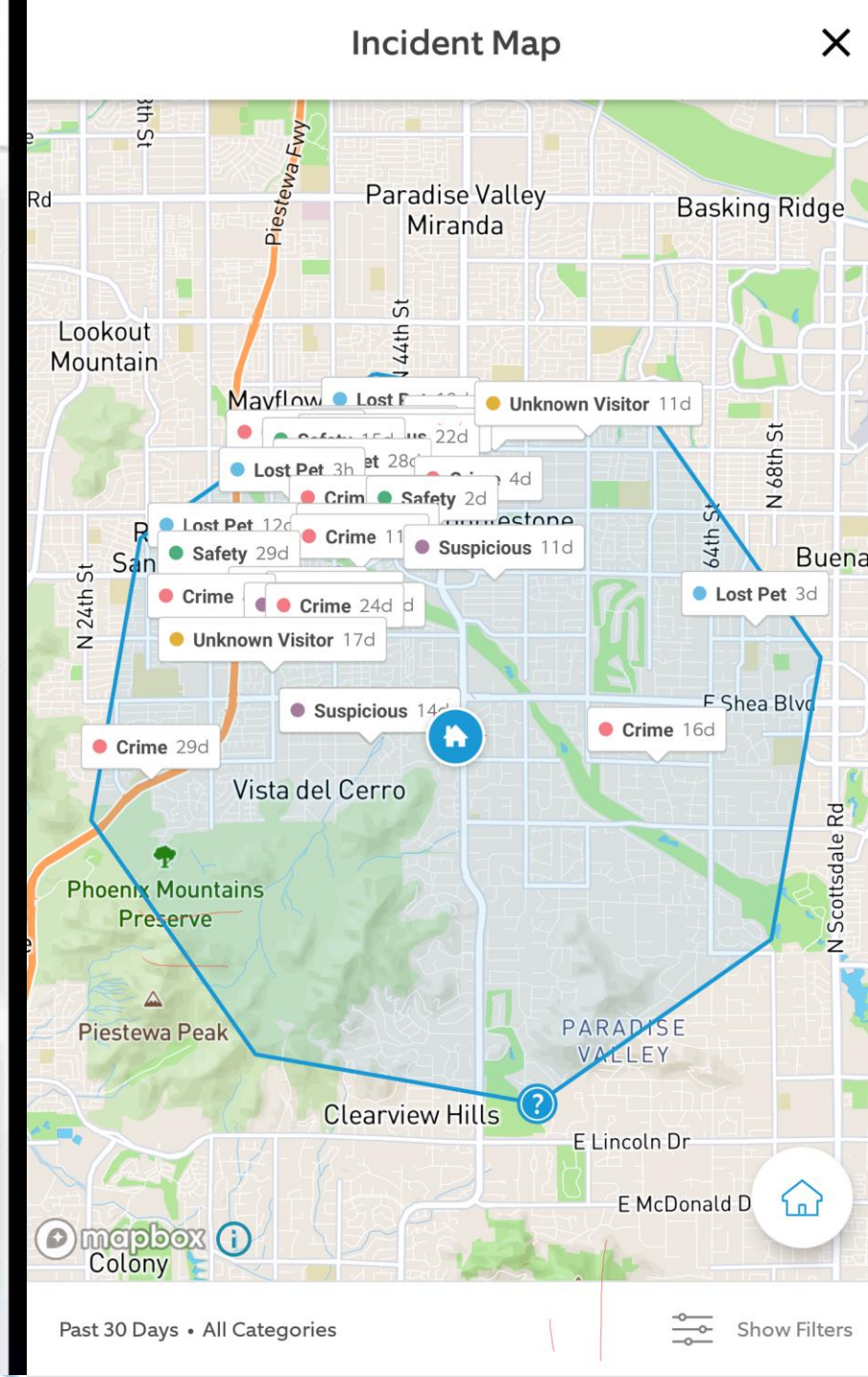
Next Steps for these Ring Neighborhoods

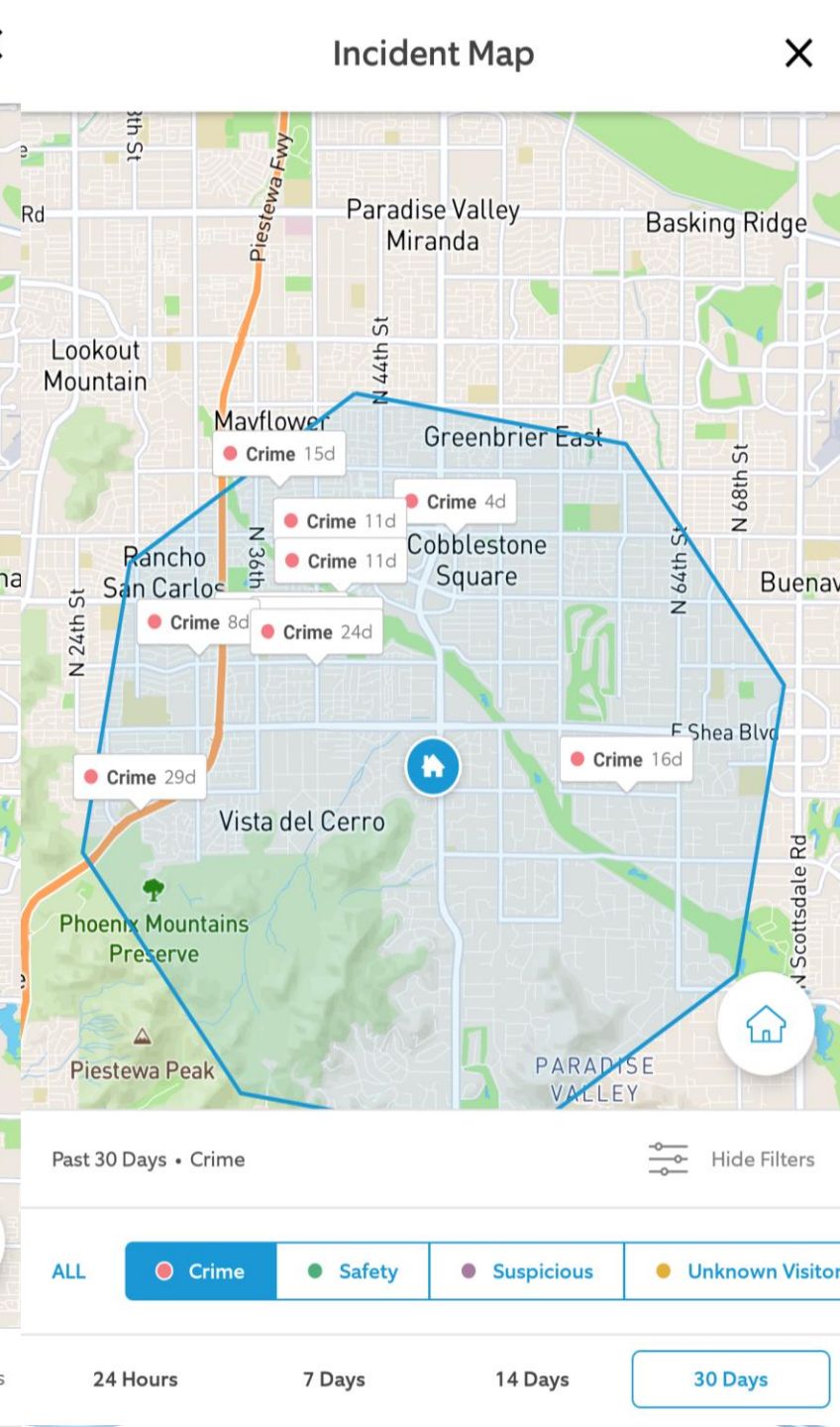
- Sen. Markey gave Ring until September 26 to answer questions on information requests but also to data retention and sharing policies, as well as other privacy concerns.
- "How long has Ring prompted its users to share video footage with law enforcement?" Markey asked Ring, pushing for a "detailed timeline of when this sharing began and how, if at all, Ring has changed its policies" over time.
- The letter asks Amazon to provide a list of all law enforcement agencies that have ever had or currently have access to Ring video
- The letter asks if Ring requires police departments to delete users' footage after a certain period, if Ring requires police departments to handle footage to minimize the risk of data breaches or leaks or control of third party footage.
- List of criminal justice and civil liberties consultants Ring has consulted in its work.

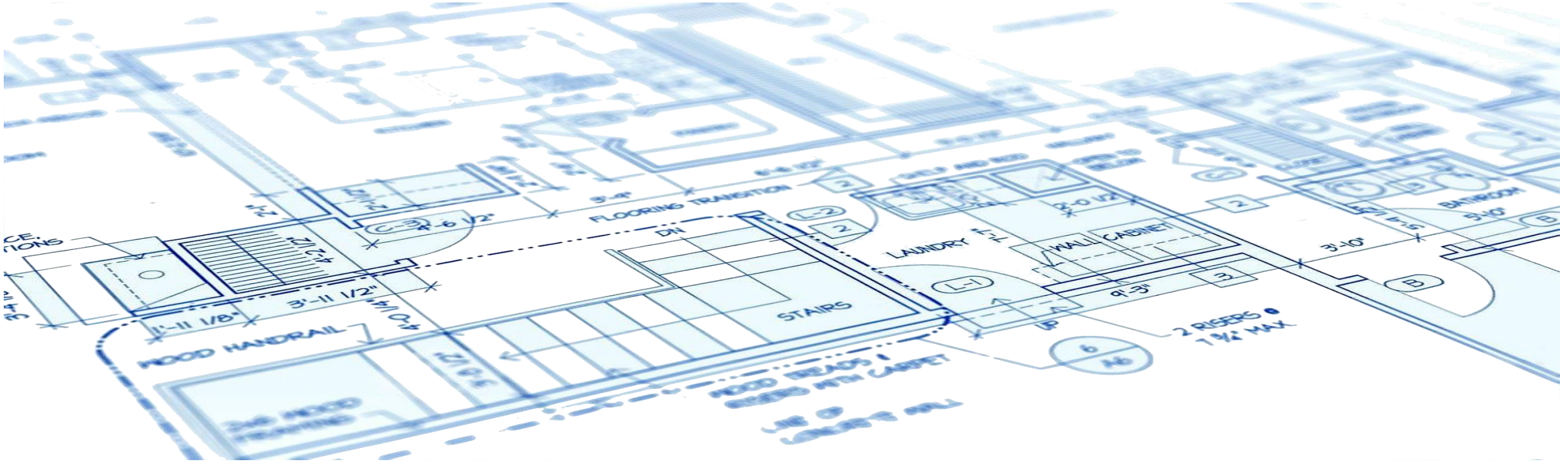


What we need is a plan…for a Code of Conduct


75°
22% 18:21
Paradise Valley Village
MAP
Neighbor
Lost Pet
2.5 miles away
STRAY DOG
Wandering in our yard and porch around 5:22am.
3 hours ago
5
1
226 Views
Helpful
Comment
Share
Neighbor
New Alert


Incident Map
Paradise Valley
Miranda
Basking Ridge
Lookout
Mountain
Piestewa Fwy
N 44th St
N 68th St
N 24th St
Unknown Visitor 11d
Lost Pet 3h
Safety 2d
Lost Pet 12d
Safety 29d
Crime 11
Suspicious 11d
Crime
Crime 24d
Unknown Visitor 17d
Lost Pet 3d
Suspicious 14d
Crime 29d
Crime 16d
Vista del Cerro
Phoenix Mountains
Preserve
Piestewa Peak
PARADISE
VALLEY
Clearview Hills
E Lincoln Dr
E McDonald D
N Scottsdale Rd
mapbox
Colony
Past 30 Days • All Categories
Show Filters


Incident Map
Paradise Valley
Miranda
Basking Ridge
Lookout
Mountain
Piestewa Fwy
N 44th St
N 68th St
N 24th St
Mayflower
Greenbrier East
Crime 15d
Crime 4d
Crime 11d
Crime 11d
Rancho
San Carlos
Cobblestone
Square
Crime 8d
Crime 24d
Crime 29d
Crime 16d
Vista del Cerro
Phoenix Mountains
Preserve
Piestewa Peak
PARADISE
VALLEY
N Scottsdale Rd
Past 30 Days • Crime
Hide Filters
ALL
Crime
Safety
Suspicious
Unknown Visitor
24 Hours
7 Days
14 Days
30 Days



Intro to Differential Security

A1 Acquisition – security sensor active, security data is created and transmitted
A2 Aggregation – Data from multiple, different sources is combined and stored
A3 Analysis (AI step 1) – Data analytics activated, neural network process active, first data visualization presented
A4 Assignment of security task (AI step 2) – First pass recommendation made; feedback on security task assignment made, neural network process active, data visualization updated
A5 Action – security response

ESS with minimal device differentiation; primarily IP video cameras

Advantages

MULTIPLE DESIGN PARAMETERS TO LEARN
OPPORTUNITY FOR IMPROVED EXPERTISE ON DIFFERENT USE CASES

HOMOGENEOUS DESIGN
SINGLE DESIGN APPROACH EASILY REPLICATED

RICH DATA AVAILABLE
VIDEO, AUDIO & METADATA

Disadvantages

MULTIPLE DESIGN PARAMETERS TO LEARN
CAMERA SYSTEM DESIGN APPLIES PRINCIPLES OF LIGHT, IMAGING RESOLUTION, OPTICAL FIELD OF VIEW, AUDIO, DIGITAL MULTIMEDIA STORAGE

HOMOGENEOUS DESIGN
KNOWLEDGE OF COMMON DESIGN APPROACHES BY HUMAN THREATS INCREASES VULNERABILITY

ICT REQUIREMENTS
HIGHER PAYLOAD INCREASES BANDWIDTH & MAKES LOW LATENCY RESPONSE ON CRITICAL USE CASES DIFFICULT; VLAN OR NETWORK SLICING REQUIRED

HIGHER POWER REQUIREMENTS
HIGHER POE LEVEL; FEW OPPORTUNITIES FOR MULTIPLE SELF POWERED DEVICES (BATTERY USAGE)

HIGHER FINANCIAL SUSTAINABILITY
MORE COMPLEX PREVENTATIVE MAINTENANCE, FIRMWARE UPDATE COMPATIBILITY CHECKS, HIGHER REPLACEMENT COSTS

POTENTIAL PRIVACY ISSUES
PUBLIC VSS SYSTEMS HAVE A HISTORY OF OPPOSITION FROM PRIVACY ADVOCATES

OBJECT RECOGNITION REQUIREMENTS
LICENCING COSTS FROM VIDEO ANALYTICS REQUIRED FOR OBJECT DETECTION & RECOGNITION ALGORITHMS; POTENTIAL FIRMWARE UPGRADE CONFLICTS

ESS with device differentiation; using IP video cameras, space protection with RADAR and/or LiDAR, non-video object recognition using LiDAR

Advantages

MULTIPLE DESIGN PARAMETERS TO LEARN
OPPORTUNITY FOR IMPROVED EXPERTISE ON DIFFERENT USE CASES WITH DIFFERENT DEVICE CATEGORIES

DIFFERENTIAL DESIGN
ROBUST DESIGN APPROACH REDUCES RISK, IMPROVES ACCURACY OF THREAT IDENTIFICATION

RICH DATA AVAILABLE
VIDEO, AUDIO & METADATA, OBJECT(S) LOCATION, OBJECT RECOGNITION

OBJECT RECOGNITION INCLUDED
OPEN SOURCE SOFTWARE SUPPORTS LIDAR SENSORS, IDENTIFIES POINT CLOUDS AS PEOPLE, VEHICLES, FOLIAGE, BUILDINGS, ROADS, STRUCTURES

ICT REQUIREMENTS
LOWER PAYLOAD DUE TO INCREASED NUMBER OF DIVERSE, LOW BANDWIDTH DEVICES LIKE LIDAR AND RADAR

LOWER POWER REQUIREMENTS
MULTIPLE POE CLASSES USED; SOME DEVICES MAY BE USED SELF POWERED DEVICES (BATTERY USAGE)

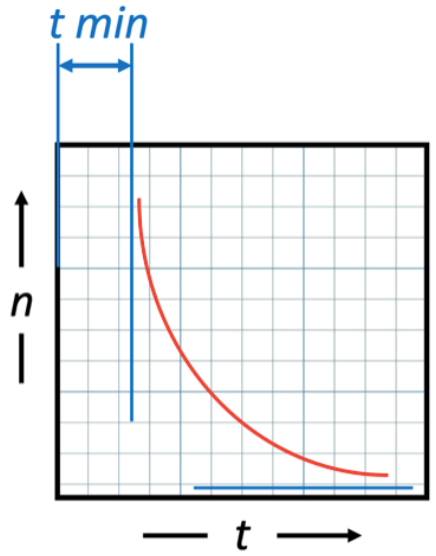
LESS PRIVACY ISSUES
LESS IP VIDEO CAMERAS REDUCES PRIVACY ISSUES; LIDAR OBJECT RECOGNITION DONE WITHOUT REVEALING OBJECT DETAILS; PRESERVES PRIVACY

Disadvantages

MULTIPLE DESIGN PARAMETERS TO LEARN
CAMERA SYSTEM DESIGN APPLIES PRINCIPLES OF LIGHT, IMAGING RESOLUTION, OPTICAL FIELD OF VIEW, AUDIO, DIGITAL MULTIMEDIA STORAGE, LIDAR SPACE PROTECTION DESIGN

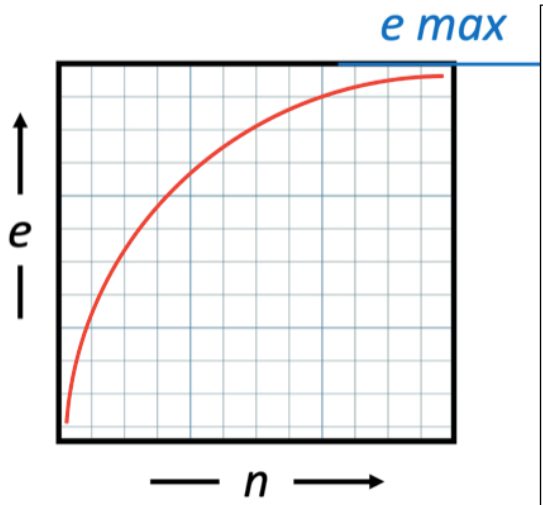
DIFFERENTIAL DESIGN
COMPLEXITY OF MULTIPLE IOT DEVICES

Variable	Description
n	Quantity of IoT sensors
e	Detection Efficiency
d	Differentiation or Randomness of IoT sensors
c	Total or projected cost of IoT sensors



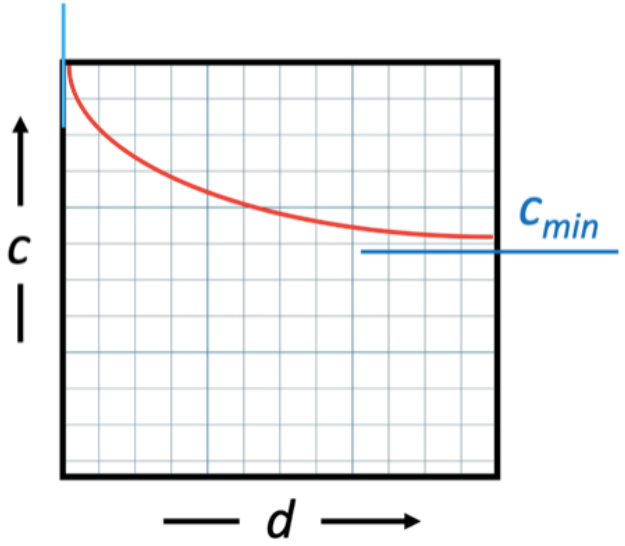
The number of devices and the average ESS response time are inversely related. With a greater number of devices added to the ESS using DiffSec, a minimum response time is approached, but never reached.

$$\lim_{n\to\infty} t = t\ min$$



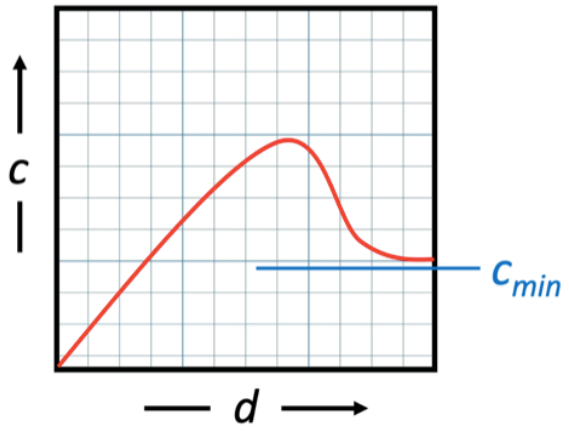
As the number of differentiated devices is added, the average efficiency of ESS response time approaches a maximum.

$$\lim_{n\to\infty} e = e\ max$$



As the amount of differentiation in the ESS increases, the average device cost approaches a minimum

$$\lim_{d \to \infty} c = c\ min$$



As the ESS contains more differentiated devices and its differentiation increases, the average cost per device varies until it begins to approach a minimum.

$$\lim_{d \to \infty} c = c\ min$$

	SEIM	PSIM	VMS	CAD	SCADA	ERM	XaaS	V2X
Meaning	Security Event Information Management system (information technology/security)	Physical Security Information Mgt	Video Mgt System	Computer-aided Dispatch	Supervisory control and data acquisition	Enterprise Risk Mgt	Everything as a Svc	Vehicle to everything
Description	Combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.	Integrates multiple security applications and devices to control them through one comprehensive user interface	System to record, playback perform data queries & Manage Digital Multimedia Content (IP video, audio and metadata)	Used by emergency communications dispatchers, call-takers, and 911 operators in centralized, public-safety call centers, as well as by field personnel; Data transmitted to first responders includes location, reporting party and incident	System of software and hardware elements that allows industrial organizations to: Control industrial processes locally or at remote locations. Monitor, gather, and process real-time data	Provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process.	cloud-computing providers offer their "services" according to different models, of which the three standard models per NIST are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)	passing of information from a vehicle to any entity: V2I (vehicle-to- [traffic & transportation] infrastructure, V2N (vehicle-to-network), V2V (vehicle-to-vehicle), V2P (vehicle-to-pedestrian), V2D (vehicle-to-device) and V2G (vehicle-to-grid).
DiffSec impact & compatibility	High impact & compatibility	Limited processing of transportation, process control, life safety and environmental sensors	Limited processing of transportation, process control, life safety and environmental sensors	Requires sensor processing applications	High impact & compatibility	Requires sensor processing applications	Widest data ingestion possible over virtual delivery of services. Requires sensor processing applications	High impact; average compatibility. V2I is primary focus where video surveillance, acoustic sensors, LiDAR, LPR devices are connected in smart city & traffic applications

SURFARO LLC

SERVICES

DESIGN ▪ PROJECT MANAGEMENT ▪ STANDARDS COMPLIANCE

TECH FOCUS

INTELLIGENT BUILDINGS ▪ PHYSICAL INFRASTRUCTURE ▪ SECURITY/SAFETY ▪ VIDEO ANALYTICS ▪ ACCESS CONTROL ▪ FIRE/LIFE SAFETY ▪ MASS NOTIFICATION ▪ COMMAND CENTERS