

WEEK 1

# Foundations of Cyber Ethics and Law



# Today's Agenda



## Foundations

What cyber ethics and cyber law are, and why the field exists



## Why Ethics Matters in Security

The unique stakes of a profession built on privileged access



## Ethical Frameworks

Five lenses for reasoning through hard calls



## Professional Responsibility

Duties to employers, the public, and the profession



## Legal vs. Ethical vs. Policy

Telling four kinds of obligation apart



## Case Study: Flock Cameras

Applying every framework to a live, unresolved controversy



## Group Activity

Case analysis, debate, and debrief



#### OPENING QUESTION

*“Can something be perfectly legal and still be wrong?  
Can something violate policy but still be the right thing to do?”*



## SECTION 1

# Foundations of Cyber Ethics and Law

What ties law and ethics together — and what pulls them apart

# Two Related, Distinct Fields



## Cyber Ethics

The branch of applied ethics concerned with moral behavior in computing and information technology.

Asks: how people and organizations OUGHT to act with respect to data, systems, privacy, and digital harm.



## Cyber Law

The body of statutes, regulations, and case law governing conduct in digital and networked environments.

Asks: what people and organizations are LEGALLY required or prohibited from doing.

***The key distinction: law tells you the floor. Ethics often asks for more than the floor.***

# Why Cyber Ethics Is Its Own Discipline



## Technology outpaces law

Legislation takes years; new tools, platforms, and attack techniques emerge in months. Professionals routinely face situations the law hasn't addressed yet.



## Harms are often invisible

A breach's victims may never know they were affected. Diffuse, delayed harm is much harder to hold anyone accountable for than physical-world harm.



## Privileged access raises the stakes

IT and security professionals routinely have access to data and systems most professions never touch — which multiplies the ethical weight of ordinary daily decisions.

# Historical Anchor Points





## SECTION 2

# Why Ethics Matters in Cybersecurity

The unique stakes of a profession built on trust and access

# Security Is a Trust Profession First

*Every other engineering discipline builds things. Security professionals are handed the keys to things other people built — and asked not to misuse them.*



## **Asymmetric access**

Security staff can often read emails, monitor traffic, access financial systems, and see data no one else in the organization can see.



## **Asymmetric knowledge**

Most people can't evaluate whether a security decision was reasonable. Clients and the public must trust professional judgment they cannot independently verify.



## **Asymmetric consequences**

A single unethical or careless decision — a leaked database, an unpatched system, a misused surveillance tool — can affect thousands of people who never consented to the risk.

## WHAT'S AT STAKE WHEN ETHICS FAILS



### **Public trust**

Erodes fastest — and is the hardest thing in security to rebuild once lost.



### **Legal exposure**

Regulatory fines, lawsuits, and consent decrees often follow ethical failures before criminal ones.



### **The profession's credibility**

One high-profile misuse of access reinforces public suspicion of the entire field.



### SECTION 3

# Ethical Frameworks

Five lenses professionals use to reason through hard calls

# Five Lenses, Not Five Competing Answers

*Professionals often use more than one framework when reasoning through a genuinely hard case. Think of these as lenses to look through, not a checklist to pick from.*



## Utilitarianism

Judge by outcomes — the greatest good for the greatest number.



## Deontology

Judge by duty — does the action follow a moral rule, regardless of outcome?



## Virtue Ethics

Judge by character — what would a person of integrity and prudence do?



## Rights-Based Ethics

Judge by rights — some claims (privacy, autonomy) hold even against the greater good.



## Social Contract Theory

Judge by agreement — obligations arise from the implicit terms between parties.

# Utilitarianism



*Greatest good for the greatest number*

## SCENARIO PROMPT

Is it justified to monitor employee communications if doing so prevents a breach that would harm thousands of customers?

A utilitarian weighs total benefit against total harm, across everyone affected — not just the parties in the room.

# Deontology



*Duty-based ethics (associated with Kant)*

## SCENARIO PROMPT

Even if disclosing a vulnerability might cause short-term harm before a patch exists, is there a duty to be honest with affected users regardless of consequences?

A deontologist asks whether an action follows a moral rule — not whether the outcome turns out well.

# Virtue Ethics



*Character over rules or outcomes*

## SCENARIO PROMPT

What habits of integrity, discretion, and prudence should a security professional cultivate — independent of any single decision?

A virtue ethicist asks what a person of good character would do, trusting that character to generalize across situations rules can't anticipate.

# Rights-Based Ethics



*Some claims hold regardless of the greater good*

## SCENARIO PROMPT

Do individuals have a right to control their own data — a right that shouldn't be overridden even if sharing that data would benefit others?

This is the framework behind most privacy law: certain rights (privacy, autonomy, due process) are treated as not up for a cost-benefit trade.

# Social Contract Theory



*Obligations arise from implicit agreement*

## SCENARIO PROMPT

Terms of Service and end-user agreements attempt to formalize a social contract between companies and users.

Push students to ask: is this really 'agreed to' when most people never read what they're accepting?

# One Scenario, Five Lenses

*A company discovers a vulnerability that's actively being exploited. Disclosing it publicly will hand attackers a roadmap before a patch is ready.*

## Utilitarianism

Weigh total harm of exploitation vs. total harm of delayed disclosure across all users.

## Deontology

Ask whether there's a duty to inform affected users, independent of the immediate outcome.

## Virtue Ethics

Ask what a professional of integrity and prudence would do in this exact position.

## Rights-Based

Ask whether users have a right to know about risks to their own data or systems.

## Social Contract

Ask what the implicit agreement with users and the security community actually promises.



#### SECTION 4

# Professional Responsibility

Duties that extend well beyond 'don't break the law'

# Four Duties, Sometimes in Tension



## Duty to the Public

The broadest duty, and the one most codes open with — “contribute to society and human well-being.”



## Duty to Employers & Clients

Competence, honesty, confidentiality, and avoiding conflicts of interest.



## Duty to the Profession

Maintaining the credibility of the field as a whole — why credentialing bodies revoke certifications for violations.



## Duty to Colleagues

Fair treatment, honest collaboration, and mentorship within teams.

# When Duties Collide: Whistleblowing



ACM Code of Ethics

**Whistleblowing is where duties most directly conflict:**

## **Duty to Employer**

Confidentiality, loyalty, and the terms of employment pull toward staying silent.

## **Duty to the Public**

Most professional codes hold that this takes precedence — but rarely without legal risk, retaliation, or uncertainty about the severity of harm.



## SECTION 5

# Legal, Ethical, Policy & Organizational Requirements

The conceptual core of the course — four kinds of obligation, easily conflated

# Four Categories of Obligation

| Category      | Source of Authority                        | Enforcement                                    | Example                                                   |
|---------------|--------------------------------------------|------------------------------------------------|-----------------------------------------------------------|
| Legal         | Government (statute, regulation, case law) | Courts, fines, criminal penalties              | HIPAA requires breach notification within a set window    |
| Ethical       | Moral reasoning, professional norms        | Conscience, professional community, reputation | Disclosing a flaw to users even when not legally required |
| Policy        | An organization's internal rules           | HR action, termination, internal discipline    | A company ban on personal USB drives on work machines     |
| Best Practice | Industry consensus, standards bodies       | Certification, market pressure, insurance      | Following NIST or ISO 27001 where not legally mandated    |

# The Space Between Categories

## Legal, but Unethical

A company may legally sell user data under a technically-compliant privacy policy that almost no user actually read or understood.

## Illegal, but Arguably Ethical

Some historical cases of researchers publicly disclosing vulnerabilities against a company's wishes, prioritizing public safety over compliance.

## Against Policy, but Ethical

An employee reporting a colleague's misconduct through a channel that technically violates a confidentiality policy.

## Compliant, but Questionable

Using dark patterns in UI design that are technically disclosed in the terms of service but built to obscure real user choice.



## SECTION 6

# Case Study: Flock Cameras & Rising Surveillance

A live, unresolved controversy — and a perfect test of everything covered so far

# What Is Flock Safety?



## **AI-enabled license plate readers**

Cameras that scan and log every vehicle that passes — plate number, make, model, color, and even bumper stickers and scratches — cataloged automatically by AI.



## **A nationwide, interconnected network**

Over 6,000 customer communities across nearly every U.S. state, with roughly 80,000+ cameras feeding into shared, searchable databases.



## **Sold as a public-safety tool**

Marketed to local governments as a force multiplier for law enforcement — recovering stolen vehicles, solving crimes, locating missing people.

## What Supporters Point To

**~10%**

of reported U.S. crime, Flock claims, is solved in part using its technology (a figure critics — including Flock's own researchers — have disputed).

**250+**

stolen vehicles recovered at least in part through Flock's system in Denver alone, along with evidence in nine homicide arrests.

**6,000+**

communities under contract nationwide — evidence the product remains popular with many local governments and police departments.

# What Critics Point To



## Warrantless mass tracking

Civil rights advocates argue the system violates the Fourth Amendment's prohibition on unreasonable searches — a federal judge has called it “an unsettled area of law.”



## Accuracy failures with real consequences

In New Mexico, misread plates led police to hold innocent drivers at gunpoint. An Ohio man was wrongly identified as a human trafficking suspect in a since-dismissed lawsuit.



## Mission creep beyond ‘crime-fighting’

Reporting has tied the shared national database to immigration enforcement use — far outside the original stolen-vehicle-and-violent-crime pitch made to city councils.

# The Backlash Is Escalating

1

## Property damage & protest

Cameras cut down with saws in upstate New York, doused in paint in Oakland, and rammed by a truck in Idaho; one Florida resident blocks a camera with a cardboard sign on a lawn chair.

2

## Local governments pulling out

Santa Cruz, Mountain View, El Cerrito, and Chandler have ended or declined to renew Flock contracts in 2026 after sustained community organizing.

3

## Company countermeasures

In August 2026, Flock announced new guardrails — mandatory case-number labeling for searches, automatic abuse review, and a default data-retention window cut from 30 days to 7.

# Running Flock Through Today's Framework

## Legal

Fourth Amendment status is unresolved and actively being litigated — a genuine gray zone, not settled law.

## Ethical

Apply utilitarian (public safety benefit) vs. rights-based (privacy as a claim that shouldn't be traded away) reasoning — they point in different directions.

## Policy

Cities set their own retention, sharing, and immigration-search policies — which is exactly why some communities kept Flock and others didn't.

## Professional Responsibility

Security and civic-tech professionals who build or deploy this technology hold real duties to the public whose movements are being logged without their knowledge.

## CLASS DISCUSSION

# Discuss Before We Move to the Activity



Should a technology's legal status (“unsettled”) change how comfortable your city should be deploying it?



Whose consent actually matters here — the city council that signs the contract, or the residents who are recorded without being asked?



Is “we'll add safeguards after the backlash” a responsible pattern for deploying surveillance technology, or a warning sign?



If you worked for Flock, what professional duties would you feel toward the public whose data flows through your product?



## SECTION 7

# Group Activity: Case Study Analysis

Apply everything from today to a realistic professional dilemma

# Case Study Analysis — Instructions

*Scenario: A security researcher discovers a serious vulnerability, reports it privately, gets no response for months, and is weighing public disclosure against the company's wishes.*

- 1 Legal analysis — what does the law require or prohibit? Where's the ambiguity?
- 2 Ethical analysis — apply at least two frameworks from today. Do they agree?
- 3 Policy analysis — what organizational policy (NDA, disclosure policy) is in play?
- 4 Professional responsibility — whose interests should take priority, and why?
- 5 Recommendation — what should this person do? Name the strongest counterargument.

*Groups of 3–4 · 35 minutes to analyze · 15 minutes to debrief*

# Debrief — What We're Listening For



## **Disagreement is the point**

Ask groups with different recommendations to defend their reasoning to each other. Consensus isn't the goal — sound reasoning is.



## **'It depends' is a legitimate answer**

When justified with real reasoning across all four categories, this is what professional judgment sounds like — not a dodge.



## **Setting up next week**

This activity previews a deeper dive into the legal framework, now that ethical reasoning has been established as the throughline for the course.

## KEY TAKEAWAYS

# What to Carry Into Every Case From Here On



Law is the floor. Ethics frequently asks for more than the floor requires.



No single ethical framework has the final word — strong reasoning uses several.



Professional responsibility means duties to the public, not just to your employer.



Legal, ethical, policy, and best-practice obligations are four different things — learn to name which one you're actually arguing about.



Flock Safety shows all four categories in live tension, with no settled answer yet — which is exactly the kind of case this course exists to prepare you for.

NEXT WEEK

# The Legal Framework in Depth

Bring your case study write-up — we'll revisit it once we've added statutory detail to the legal analysis you did today.

