

AUDITS CONDUCTED UNDER ATTORNEY CLIENT PRIVILEGE

How to Manage the "ACP" Framework During an Audit Engagement

COMPLIANCE & ETHICS INSTITUTE



AGENDA

- Audits Conducted under Attorney Client Privilege (ACP)
- Break
- Cyber Audits and Litigation Risks
- Break
- Pay Equity Audits
- Q&A

AUDITS CONDUCTED UNDER ATTORNEY CLIENT PRIVILEGE

Audit Basics

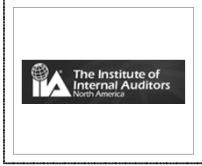
COMPLIANCE & ETHICS INSTITUTE

SCCE[™]
Society of Corporate Compliance and Ethics

AUDIT BASICS

Mission
To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.


- Mandatory guidance
- Definition of internal audit
- Code of Ethics
- Standards



SCCE[™]
Society of Corporate Compliance and Ethics

COMPLIANCE & ETHICS INSTITUTE

AUDIT BASICS



Core Principles

Demonstrates integrity.

Demonstrates competence and due professional care.

Is objective and free from undue influence (independent).

Aligns with the strategies, objectives, and risks of the organization.

Is appropriately positioned and adequately resourced.

Demonstrates quality and continuous improvement.

Communicates effectively.

Provides risk-based assurance.


Is insightful, proactive, and future-focused.

Promotes organizational improvement.

SCCE[™]
Society of Corporate Compliance and Ethics

COMPLIANCE & ETHICS INSTITUTE

AUDIT BASICS




Standards

1100 – Independence and Objectivity
The internal audit activity must be independent, and internal auditors must be objective in performing their work.


1300 – Quality Assurance and Improvement Program
The chief audit executive must develop and maintain a quality assurance and improvement program that covers all aspects of the internal audit activity.

1312 – External Assessments
External assessments must be conducted at least once every five years by a qualified independent assessor or assessment team from outside the organization.


SCCE
 Society of Corporate Compliance and Ethics

COMPLIANCE & ETHICS INSTITUTE

AUDIT BASICS


The Institute of Internal Auditors
 North America

Standards
 1100 – Independence and Objectivity
 1300 – Quality Assurance and Improvement Program
 1312 – External Assessments

Practical Tip: Consider how these standards and obligations can affect ACP work or work product.


- When deciding on an ACP project can Counsel's oversight impact Audit's independence?
- How are your audit team's Quality Assurance Reviews (QAR) conducted and are ACP documents handled?

Practical Tip: When relying on audit for monitoring and testing of legal or compliance processes engage audit to identify / discuss ACP determination which is different than auditing processes in sensitive legal-oriented areas as part of the normal course of risk assessment for the organization.

AUDITS CONDUCTED UNDER ATTORNEY CLIENT PRIVILEGE

Attorney Client Privilege (ACP) Basics

COMPLIANCE & ETHICS INSTITUTE


SCCE
 Society of Corporate Compliance and Ethics

ATTORNEY CLIENT PRIVILEGE BASICS

| OBJECTIVE | DISCUSSION EXCLUSIONS |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> • Scope: Performing an audit engagement or audit work at the direction of counsel for purposes of giving legal advice • Protects against disclosure of communications and documents regarding confidential information while providing legal advisement • Applicable to audit work when an attorney performs the review and provides oversight of the audit work that involve legal issues | <ul style="list-style-type: none"> • Upjohn [#IAALBIANYL] • Attorney reporting obligations • Cross border privilege rules • External audit requests for information |

ATTORNEY CLIENT PRIVILEGE BASICS

Basics:

- ACP protects
 - Confidential communications (Attorney Client Communications – "ACC")
 - Attorney Work Product (Litigation)
- Ethical rules (WA)
 - RPC 1.6: Confidentiality of Information. (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
 - RPC 1.13: Organization as Client. (a) A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.
 - RPC 2.1: Advisor. In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.

ATTORNEY CLIENT PRIVILEGE BASICS

Basics:

- ACC can protect
 - Confidential communications
 - between lawyer and client
 - with the intent that it be kept confidential
 - for the primary purpose of obtaining or rendering legal advice
- ACP isn't automatic – and there are challenges
- Privilege is very narrowly construed – and the burden is on the party seeking to assert the privilege to show ACP requirements have been met
- Privilege protects communications, not the underlying facts

ATTORNEY CLIENT PRIVILEGE BASICS

Basics:

- What are the means of communication that can be protected?
 - Oral
 - Written
 - Email
 - IM
 - Text
 - Notes
 - Presentations
 - Workpapers - e.g. spreadsheets

ATTORNEY CLIENT PRIVILEGE BASICS

Challenges:

- Comingling business (risk) advice with legal advice
- Optics: scrutiny of in house assertions (v. outside counsel)
- Optics: taking active steps to "direct" the audit activities
- Navigating role as Counsel rendering legal advice and other legal roles (e.g. Compliance Officer, Corporate Secretary, etc.)
- Limiting information to those "need-to-know" stakeholders
- Protecting documents
- Avoiding waivers

Practical Tip: Always be clear about asserting the request or issuing of legal advice

ATTORNEY CLIENT PRIVILEGE BASICS

Challenges - waivers:

- The confidential communication is shared with a third party
 - Waiver means the communication is no longer protected from disclosure
 - Waiver can be intentional or inadvertent
 - The attorney-client privilege belongs to the client (Company) and only Company executives or attorneys can intentionally waive the privilege
 - Waiver can extend to not only a specific communication, but to all communications regarding issues or subject areas discussed in the communication

How does this apply to an ACP audit?

ATTORNEY CLIENT PRIVILEGE BASICS

Challenges - waivers:

- Issuing ACP after a review/assessment commences – investigation example
 - *Premera Blue Cross Customer Data Security Breach Litigation, Case No. 3:15-md-2633-SI, 2017 U.S. Dist. LEXIS 178762 (D. Or. Oct. 27, 2017)*
 - Premera claimed privilege and work product protection for its data breach investigation. The court rejected both claims. Among many other things, the court assessed Premera's work product claim for documents created by its consultant Mandiant. Premera had hired Mandiant to review its claims data management system in October 2014. On January 29, 2015, Mandiant discovered malware on the system. Premera quickly hired an outside lawyer, and on February 21, 2015, "Premera and Mandiant entered into an amended statement of work that shifted supervision of Mandiant's [later] work to outside counsel."

AUDITS CONDUCTED UNDER ATTORNEY CLIENT PRIVILEGE

Directing Audit Engagements with Protocols

COMPLIANCE & ETHICS INSTITUTE



DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

THE "WHY"

- Compliance determinations needing legal advisement – privileged communications
- Distinguish the audit objective from:
 - Investigative purpose
 - Risk assessment activity
- **Seeking:** Audit of information or processes for purposes of rendering legal advice

THE "HOW"

- Attorney direction and oversight
- Communication & documentation protocols
- Training
- Practical guidelines: **know the limits, identify and address risks**

COMPLIANCE & ETHICS INSTITUTE



DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Tactical questions:

- Who is performing the audit work? Internal audit or is this a co-source audit?
- Who is supervising the audit work? In house counsel or outside counsel?
- As in house counsel, do you have time to "direct" the audit work or does this require outside counsel oversight? [ethics reminder]
- Do your audit teams – whether internal audit or external firm – understand ACP standards?

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Document audit/risk assessment ACP protocols (recommended):

- Clearly explain the purpose of any guidelines as it pertains to protecting attorney client and work product privileges

These guidelines outline the process for designating and protecting the confidentiality of internal audits and risk assessments performed in anticipation of litigation under the attorney work product doctrine and/or for the purpose of providing legal advice under the attorney client privilege.

The attorney client privilege protects and encourages confidentiality when a client seeks, or an attorney provides, legal advice in a confidential manner. These guidelines explain how to ensure that the privilege applies and that communications reflect that intent.

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Documented protocols, continued:

- Include attorney oversight directions
 1. Establish who is directing the work and acting as the single point of contact for Legal
 2. Issue a memo to document the audit engagement, as in house counsel overseeing the work
 3. Identify additional attorney legal SMEs given scope
 4. Fundamental responsibilities: direct the work, control the communications, uphold ACP protections, render legal advice

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Documented protocols, continued:

- Audit engagement notification and planning directions to audit staff
 1. Notification memo
 2. Initial planning meeting and ACP guideline overview
- Communications protocols
 1. General directions – limiting communications and upholding confidentiality
 2. Email guidance – general headers and ACP language
 3. Requests for information – guidance and oversight of “exchanges”

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Documented protocols, continued:

- Interviews
 1. The purpose of the interview is to collect information as part of an audit requested by Legal counsel
 2. The interview is protected under the attorney-client privilege, and
 3. The privilege is held by the Company, not the interviewee
 4. The interviewer should keep the substance of the interview confidential.
 5. Handout materials should be marked "ACP" and collected by the interviewer at the end of the interview if shared to facilitate discussion, etc.

Does Legal counsel need to be present at interviews?

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Documented protocols, continued:

- Documentation and storage instructions
 1. Interview materials
 2. Records (work papers, testing samples)
 3. Audit work paper storage:
 - Internal audit repository
 - Secure shared/collaboration site (Legal)
 - Outside counsel or co-source* network locations

Do co-source (third party) auditors receive company-issued equipment?

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Documented protocols, continued:

- Written report writing / process guidelines
 1. Document mechanics
 - "ACP" designation
 - Slide footer and cover page
 2. Draft reviews (soft copy)
 3. Revisions and action owner communications
 4. Final report and distribution

Can the audit engagement team issue the final report?

Privileged and Confidential.
Property of the reporter of course.
Reproduction by any means is prohibited without the prior written consent of the reporting firm.

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

Documented protocols, continued:

- Audit Committee communications and “package” – consider -
 - The Audit Committee’s need to know given their oversight requirements and charter
 - Whether an attorney can provide a read out of the report or issues requiring legal advice
 - Coordinating with the audit function

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

2. ACP overview and training:

- Provide the necessary training or explaining to audit engagement teams on how to preserve the privilege and Counsel’s role
 - Standard ACP notifications given at meetings (e.g. performing audit at the direction of Counsel, information discussed is confidential and not to be shared or distributed, contacting Counsel with questions or requests, etc.)
 - Communication practices: avoiding pitfalls like requests for information or process inquiries in long email exchanges under ACP

DIRECTING AUDIT ENGAGEMENTS - PROTOCOLS

3. For audit co-source engagements:

- Include the ACP directive in MSA/SOW terms:
 - Auditing at the direction of counsel for purposes of giving advice
 - Communication protocols: workpapers, report, communications
- Counsel inclusion in “Kick-off” and status meetings
- Continue to clarify roles and “Directing Counsel’s” responsibility to provide oversight by directing work, reviewing drafts, etc.

AUDITS CONDUCTED UNDER ATTORNEY CLIENT PRIVILEGE

Practical Guidance

COMPLIANCE & ETHICS INSTITUTE



PRACTICAL GUIDANCE

- Deciding whether to conduct an Audit under ACP is a *risk-based call*
- Litigation matters and "work-product" might incur heightened burden and risk
- Controlling the communications stream for large engagements is challenging – ensure you are closely reviewing communication practices and exchanges
- Meet with the audit engagement team to provide oversight and direct work
- Issue initial "ACP" memo and provide periodic reminders to audit staff/team

COMPLIANCE & ETHICS INSTITUTE



PRACTICAL GUIDANCE

- Develop "ACP" audit memo headers – in **red** – for use during report distribution or audit engagement related communications
- Don't forget to remind people not to share in a shared file folder/SharePoint or shared application location
- Consider the technical aspects of ACP audit documentation storage and any IT governance processes needed to protect documents (QAR process, IT change management or backup processing, etc.)
- Meet with Audit prior to their Audit Planning to identify engagements that may fall within ACP [e.g. assess litigation risks for existing matters]

BREAK #1

AUDITS CONDUCTED UNDER
ATTORNEY CLIENT PRIVILEGE

Cyber Audits and Litigation

CYBER MATURITY ASSESSMENT: BASICS

What is a CMA?

An Assessment of organization's ability to
protect information assets and its
preparedness against cyber threats.

CYBER MATURITY ASSESSMENT: BASICS

What Do CMAs involve?

- (1) A standard:
 - National Institute of Standards and Technology (NIST)
 - Industry Best Practices
 - Proprietary Frameworks like KPMG and RSA
- (2) A review of the organization's people, policies and systems
- (3) A score – how well does the organization live up to the standards?

Table 1: Function and Category Unique Identifiers

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|----------------------------|----------|----------------------------|-------------------------------------------------|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management and Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| | | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| DE | Detect | DE.DP | Detection Processes |
| | | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| RS | Respond | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| | | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| RC | Recover | RC.CO | Communications |

• Source: NIST Cybersecurity Framework (April 16, 2016)

Leadership and Governance

Board demonstration due diligence, ownership and effective management of risk

Information Risk Management

The approach is designed to achieve effective risk management of information throughout the organisation and its delivery and supply partners

Operation and Technology

The level of control measures implemented to address identified risks and reduce the impact of compromise

Human Factors

The level and integration of a security culture that empowers and helps to ensure the right people, skills, culture and knowledge

Business Continuity and Crisis Management

Preparations for a security event and ability to prevent or reduce the impact through successful crisis and stakeholder management

Legal and Compliance

Regulatory and international certification standards as relevant

• Source: KPMG Cyber Maturity Assessment Model

CYBER MATURITY ASSESSMENT: BASICS

Why conduct a CMA?

PROACTIVE:

- To ensure compliance with regulations and statutes (HIPAA, CPNI)
- Meet the needs of a growing company

REACTIVE:

- Vendor Assessments
- Consent Decree
- Post-Incident Review

TO ACP OR NOT TO ACP?

"IT'S CALLED DISCLOSURE!"

How might a CMA become public?

- Civil lawsuits (discovery)
- Regulatory Investigations (FCC, FTC, AGs)
- Deal Disclosures (Due Diligence)

CONGRESSIONAL HEARINGS





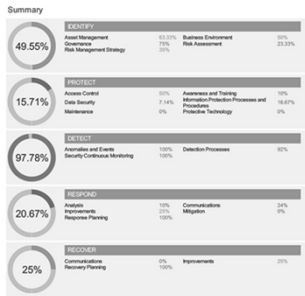
THE GOOD, THE BAD, AND THE UGLY

- Facts cannot be ACP-wrapped, so what's the big deal?
- CMAs contain characterizations of facts.
- CMAs are designed to push improvement → CMAs contains "bad" and "ugly" characterizations.
- Periodic CMAs track (lack of) progress

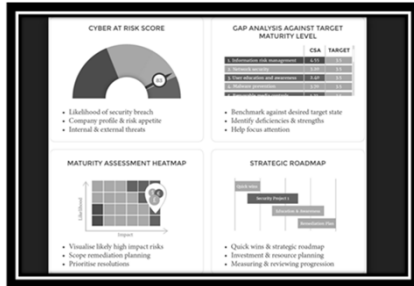
Table 7. Example Current Maturity Rating

| Capability Criteria | Evidence | Maturity Rating |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| Process and Analytics | <ul style="list-style-type: none"> Workforce planning processes at both the HQ and at sub-organization level HQ issued a data call to sub-organizations on cybersecurity workforce before making a strategic Supply and Demand Data exist and is used, but the process is arduous and there is some questions about its accuracy due to lag time | |
| Integrated Governance | <ul style="list-style-type: none"> Workforce planners sit in the Human Capital offices at HQ and sub-organizational level During a significant re-org, leadership put out guidance on how to manage and realign the cybersecurity workforce so that it would experience as little disruption as possible HQ issued a data call to sub-organizations on cybersecurity workforce before making a strategic | |
| Skilled Practitioners and Enabling Technology | <ul style="list-style-type: none"> Workforce planners sit in the Human Capital offices at HQ and sub-organizational level Workforce planners receive training on some supply and demand analysis There are no established communication channels between workforce planners; sharing information is not a common practice Systems exist, but the process is cumbersome because WF planners have to weed through several systems and databases WF planners manually update their data | |

SOURCE: Dept of Homeland Security, *Cybersecurity Capability Maturity Model White Paper* (Aug 4, 2014)



Source: Willis Towers Watson, *Cyber Risk Profile Diagnostic Tool*



Source: Clarium CMA Framework

“IT’S A CUT-AND-DRY CASE OF ATTORNEY CLIENT PRIVILEGE!”*

HOW TO WRAP A CMA IN ACP

- 1. At the direction of counsel
 - Document the engagement
 - Scope the project
 - Control the communications

- 2. For the purposes of rendering legal advice
 - Advise!
 - Example: Tie specific CMA goals to regulatory compliance

*It’s never a cut-and-dry case of Attorney Client Privilege

TYING CMA TO LEGAL ADVICE

- GLBA Standards for safeguarding customer information (16 CFR § 314.3).
- Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

TYING CMA TO LEGAL ADVICE

- HIPAA Administrative safeguards 45 CFR 164.308 –
- (i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.
- (ii) **Implementation specifications:**
 - (A) **Risk analysis (Required).** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
 - (B) **Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
 - (C) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
 - (D) **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

TYING CMA TO LEGAL ADVISE

- 47 USC § 222(a) – Federal Customer Proprietary Network Information law
- 23 NYCRR 500.02(b)(1) – New York Department of Financial Services – Cybersecurity Requirements for Financial Services Companies
- 201 CMR 17.03(2) (b) -- Massachusetts "Standards for the Protection of Personal Information of Residents of the Commonwealth"
- State breach notification laws
- Consent Decree requirements

"IT'S CALLED WAIVER!"

HOW TO LOSE ACP PROTECTION

- Failing to have counsel direct the assessment
- Comingling business (risk) advice with legal advice
- Failing to provide legal advice
- Oversharing the CMA
- Incorporating CMA into non-privileged documents
- "Applying" ACP after the fact

TO ACP OR NOT TO ACP?

- Deciding whether to conduct an Audit under ACP is a risk-based call
- Is the organization facing current litigation or regulatory inquiries
- Was there a recent cybersecurity event that is likely to give rise to litigation or regulatory investigation
- Does the organization have the time, money, and resources to actually run the CMA under ACP

CMAS AS WORK PRODUCT:
SPECIAL CONSIDERATIONS

- The Work Product privileged is different from the Attorney-Client Communication Privilege
- Applies when documents are prepared by non-attorneys "because of" or in "preparation for" actual or threatened litigation.
- Courts weigh factors: timing of retention, timing of litigation holds, and, of course, direction of counsel (i.e., no potted plants)

CMAS AS WORK PRODUCT:
SPECIAL CONSIDERATIONS

- The Work Product privileged is not absolute
- Like the ACC privilege, WP may be waived.
- Unlike the ACC, "work product" docs may still be discovered if "they are otherwise discoverable under Rule 26(b)(1)" and if "the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means." Fed. R. Civ. P. 26(b)(3)(A)(i)-(ii).

CMAS AS WORK PRODUCT:
SPECIAL CONSIDERATIONS

- An Organization might conduct a CMA in response to a significant security incident.
- CMAs in these circumstances may often follow on the heels of an incident-specific investigations
- Danger that unprotected CMA could waive ACP for prior investigations

CASE STUDIES

- *In re Experian Data Breach Litig.*, Civ. No. 15-01592, 2017 U.S. Dist. LEXIS 162891 (May 17, 2017) (Protecting Post-Incident Investigative report as Work Product)
- *Genesco, Inc. v. Visa U.S.A., Inc.*, F.R.D. 559 (M.D. Tenn. 2014) (Protecting Post-Incident Investigative report as Work Product)
- *In re Anthem, Inc. Data Breach Litig.*, 236 F. Supp. 3d 150 (D.C. 2017) (Plaintiffs sought work papers and final report of Government audit of Anthem following data breach; some work papers protected but not all and not final report)

BREAK #2

AUDITS CONDUCTED UNDER
ATTORNEY CLIENT PRIVILEGE

Pay Equity Audits

PAY EQUITY AUDITS: THE BASICS



SEARCH FOR STATISTICALLY SIGNIFICANT DEVIATIONS



NEXT LEVEL REVIEW



THE RESULTS



THE REPORT



NEXT STEPS



GOALS OF A PAY EQUITY AUDIT

- Determine whether pay inequity exists that cannot be explained by neutral, bona fide factors;
- Assess litigation risk – from individuals or classes
- Determine whether an employer's current policies are creating, or contributing to these inequities;
- Take effective counter-measures



“60 MINUTES, “EVEN A “BEST PLACE TO WORK” CAN HAVE GENDER PAY DISPARITY” CBS, VIA YOUTUBE

MOST CRITICAL CONSIDERATION



SECOND MOST CRITICAL
CONSIDERATION

Confidential Document
Attorney-Client Privilege



WHERE



WHO



HOW



- INVOKE PRIVILEGE
- SCOPE LETTER
- DOCUMENTATION AND COMMUNICATION PROTOCOLS
- SCOPE MONITORING

Q&A

SPEAKER INFO

- Chelsea Dwyer Petersen – Partner, Perkins Coie
<https://www.perkinscoie.com/en/professionals/chelsea-dwyer-petersen.html>
- Katherine McDaniel – Sr. Counsel, T-Mobile
<https://www.linkedin.com/in/katherinemcdaniel/>
- Monica Reinmiller – Corp Counsel, T-Mobile
<https://www.linkedin.com/in/monica-reinmiller-7935976/>
