IT Policies Related to the Privacy of WPI Community Members

4th Faculty Meeting of AY 2021-22

December 02, 2021

Background

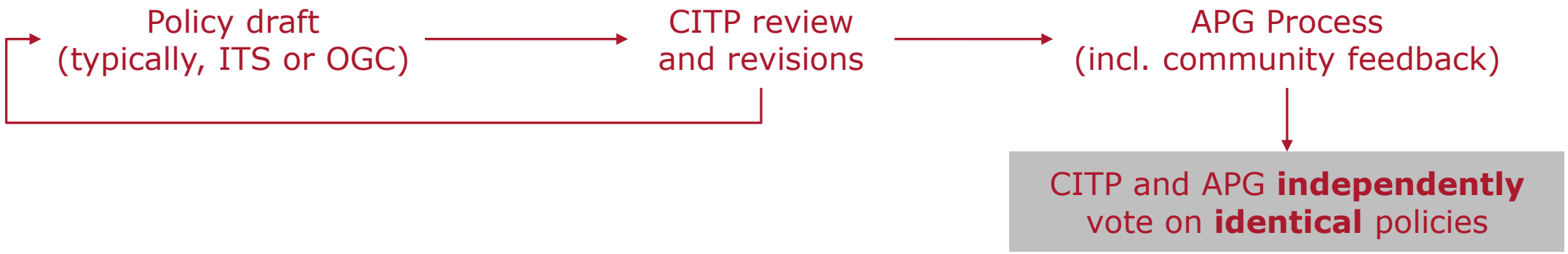
- In early- and mid-2019, the WPI Information Security, Risk, and Compliance (ISRC) Committee published a series of IT policies without formal input or approval from CITP.

- (At least) since AY 2019-20, CITP has been reviewing these policies to consider impacts on academic matters and on Faculty and student activities.

- CITP has consistently raised concerns about the potentially adverse impacts of these policies on the digital privacy of all WPI community members.

Background: CITP vis-à-vis APG

- The nature of CITP's interaction with APG continues to be problematic.
- APG lists among its members the current CITP Chair.



- This mode of collaboration was not ideal; rather, it was a working arrangement.
  - Example: Computer Systems Purchasing Policy (thanks to Prof. C. Shue).
- This mode of collaboration is no longer desired by APG.

Policies Currently under CITP Discussion

Policy Name	Published?	CITP Approved?	Status at CITP
Records Retention and Destruction Policy*	Yes Oct. 30, 2019	No	Completed two rounds of review; waiting to receive revision
Security Camera Policy	Yes Feb. 15, 2019	No	Completed two rounds of review; waiting to receive revision
Access to User Electronic Information Policy	Yes Sep. 18, 2020	No	**New** policy draft under review

- Easiest way to find currently published policy is to Google "WPI <Policy Name>"
- https://www.wpi.edu/about/policies
- *Not presented today due to limited time.

Security Camera Policy

- *"[F]ramework within which WPI will use or allow the use of Security Cameras"*
  - WPI has over 300 security cameras that record video. Two specific cameras also record audio: WPI Police interview room; Campus Center doorbell.
- CITP reviewed this policy in Spring '21, specifically Meeting #9.
- Several serious concerns were raised.
  - Definitions of Private Areas and Public Spaces
  - Notifications to occupants of Private Areas that fall under inadvertent surveillance
  - Policy on automated facial recognition
  - Access to live feeds (as opposed to recorded videos)
  - Accountability and oversight of access to video data

Security Camera Policy

- In Meeting #9 of AY 2020-21, Cheryl Martunas (Dir. Public Safety and Chief of WPI Police) clarified several matters verbally, e.g.,:
  - Primary use of security cameras was to review recorded data in Police investigations, not to monitor in real-time
  - WPI does not use automated facial recognition

- CITP recommended that the policy language should match its intent.
- Revised draft was reviewed in Meetings #1 and #2 of AY 2021-22.
  - Some issues are resolved in the revision.
  - But most of the serious concerns remain.

Concerns about Security Camera Policy

- Distinction between Public Spaces and Academic Spaces:
  - Surveillance in classrooms, labs, etc. can threaten academic freedom.
- Notification to Community members about the presence of cameras:
  - Especially when Private Areas, such as offices, fall under inadvertent surveillance; growing problem due to glass walls.
- Real-time monitoring: the policy language remains ambiguous.
- Access and retention of data: e.g., clarity regarding these issues:
  - Is anyone other than WPI Police authorized to access these data?
  - What are the procedures regarding release of these data to external agencies?
- Accountability and oversight: lack of transparency.
- See Minutes of Meeting #2 for a summary of CITP concerns.

Current Status

- CITP's concerns and requested revisions were conveyed to policy authors (OGC and WPI Police) on October 03, 2021.

- No updates on this policy have since been provided to CITP.

Access to User Electronic Information Policy

- *"[G]uidelines and processes for WPI access to User Electronic Information stored in, or transmitted through, any WPI system."*
- Policy provides a series of *"legitimate institutional purposes"* under which WPI ITS may access UEI such as:
  - E-mails including drafts and attachments, voicemails, text messages
  - Network logs; key-card access logs; wi-fi access logs
- *"Legitimate institutional purposes"* include:
  - Systems protection, maintenance, and management
  - Business continuity
  - Safety matters
  - Legal process and litigation: *"…threatened or pending litigation…"*
  - Internal investigations of misconduct
- Policy defines an *"Authorizer"* who authorizes access to UEI.

Access to User Electronic Information Policy

- CITP was reviewing a version of this policy before APG was formed.
- APG's 30-day community feedback on policy draft was May 5, 2020 – June 4, 2020.
  - From CITP 2019-20 Annual Report: *"[this] policy [proposal], too, took insufficient notice of CITP deliberations at the draft stage; it remains to be seen how much of CITP's input will be addressed in revision."*
- APG approved the policy on Sep. 16, 2020.
  - Profs. Shue and Fehribach abstained.
- CITP did not vote to approve this policy at any time.

Access to User Electronic Information Policy

- CITP began reviewing a new version of this policy in Meeting #2.
- Several serious concerns have been raised.
  - Many concerns relate to language in the existing (i.e., currently published) policy.
- General concern: the policy language leaves loopholes that make it vulnerable to abuse.
  - Therefore, the policy creates risks of violations of digital privacy of all WPI community members.
  - E.g., "*While this list is expected to cover most instances of access, the list is not intended to be exhaustive. WPI may access User Electronic Information for comparable reasons that likewise advance a Legitimate Institutional Purpose, as determined by an Authorizer…*"

(Some) Concerns about the Existing AUEIP

- Policy defines an "*Authorizer*" but does not describe who will actually access the data after AUEI is authorized.
- Section on "*Internal Investigations of Misconduct*" is disconnected from the procedures written in the Faculty Handbook and Student Code of Conduct.
- Policy language leaves loopholes that allow accessing UEI without authorization and without User notification.
- Policy includes language about oversight:
  - "*This policy, its implementation, and instances of access under this policy shall be subject to review by an Oversight Committee to be constituted by WPI, which shall include faculty and senior administrators.*"

Oversight Committee vis-à-vis Policy Implementation

- An Oversight Committee was appointed by the President.
- Current composition of Oversight Committee: Chief Information Officer, Deputy General Counsel, VP Talent & Inclusion, AVP Academic Affairs, FRC Appointee.
- The Table below is the list of *"Authorizers"* in the existing policy.

User	Legitimate Institutional Purpose				
	System Protection, Maintenance & Management	**Business Continuity**	**Safety Matters[1]**	**Legal Process and Litigation[2]**	**Internal Investigations and Misconduct**
Faculty Employee	Information Technology	Dean of department	Office of the General Counsel	Office of the General Counsel	Dean of department
Non-Faculty Employee	Information Technology	VP for Talent & Inclusion	Office of the General Counsel	Office of the General Counsel	Senior Administrator of relevant unit
Student	Information Technology	VP of Student Affairs	Office of the General Counsel	Office of the General Counsel	VP of Student Affairs

Oversight Committee Report

- Reports of the Oversight Committee are available to the WPI community.

	Time Frame	System Protection, Maintenance, Management	Business Continuity	Safety Matters	Legal Process & Litigation	Interval Investigations & Misconduct
# of Requests	9/1/20-5/31/20	N/A	9	0	6	3

- CITP was informed that many of these requests in the previous year were combined requests for a "legal hold" *and* "access."

Implications of the Oversight Committee Report

- "Legal hold" implies involuntary preservation of UEI, i.e., User cannot delete their own e-mail, drafts, OneDrive files, etc.
- Current AUEIP does not mention "legal hold" but its implementation over the last year has included legal holds.
- There seem to have been instances of access of UEI in misconduct cases, potentially in violation of Handbook procedures.
- Legal holds may have been implemented in cases not involving legal process and litigation.
- New draft policy removes the requirements for authorization, notification, and record-keeping for "routine" access. This may have already been the practice in the last year.

	Time Frame	System Protection, Maintenance, Management	Business Continuity	Safety Matters	Legal Process & Litigation	Interval Investigations & Misconduct
# of Requests	9/1/20-5/31/20	N/A	9	0	6	3

Summary and Future Actions

- CITP continues to review multiple policies that impact digital privacy of all WPI community members.
  - Policies regarding collection, retention, access, and use of electronic data pertaining to WPI community members.

- An implication of the currently published policies is that community members should have no expectation of digital privacy at WPI.

- Feedback?
  - CITP Faculty Members: R. Cowlagi, D. Petkie, G. Smith, A. Trapp