

Updated course outline: <https://people.scs.carleton.ca/~paulv/2109jan2023.html>

Common instructions and formatting for all deliverables

Upload your deliverables to Brightspace. **Due dates: see the course outline.** Timeliness rules are strict. Use **PDF format** with page margins at most 1.0 inches each, at least 11-point and at most 12-point font. One page of content is **425-500 words** for our Jan.2023 course, e.g., 40 lines averaging 12.5 words/line. (In future years, we'll use: 500-600 words.)

Avoid excessive whitespace and oversized titles (titles maximum 12 pt; use bold if emphasis desired).

Formal references (for citations). For any item you formally cite (reference), an ending references section should list the following 4 fields in the given order, separated by a period.

- 1) name of author
 - 2) title of article or book
 - 3) venue name, e.g., conference or periodical or journal or (for a book) publisher name
 - 4) publication year (add month for magazine articles, month-day for newspaper or blog articles). If an informal article lists no author, use the organization name (or as last resort, domain name) and use it also as the key for alphabetical ordering. Give a URL if there is no formal venue (e.g., for an unrefereed manuscript, whitepaper, or blog). Keep in mind that a major purpose of citations (aside from giving credit for ideas and quoted passages) is to provide enough detail for a reader to retrieve the item to cross-check the source.
-

Summary Reflections (specific instructions). Each of the 8 weekly reflections is worth 2% (16% total)

Length. **One full single-spaced page of content** (with spacing and formatting as noted above).

References if any are extra beyond this (e.g., on an extra page).

No figures or diagrams. No cover page. No abstract (instead, give context in the opening sentences).

Top line should be: COMP2109 Summary Reflection (dd-mmm-yyyy), student name + student #

Content. As a guideline, summarize 3 items that most interested you from the week's classes, comment on these items, and why they interested you. Optionally you may augment this, or replace one of these items, by items that you would have preferred that we not cover at all (and why), or explain what you would have preferred instead and why. (Keep in mind our aim to avoid duplicating content from COMP 3109 and 4108. Those courses largely follow the content in this openly accessible book:

<https://people.scs.carleton.ca/~paulv/toolsjewels.html>)

Grading rubric. The following guide will be used to assign a matching grade (full grade: 2.0):

- 2.0: suitable format, relevant class/course content, writing to the level of Gr.12 English standards
 - 1.5: short length, weak format, weak grammar/spelling, content hard to understand or not relevant
 - 1.0: seriously short or other major issues (confused content, unacceptable grammar/clarity or format)
 - 0.5: essentially nonsense or not a serious effort
 - 0.0: not handed in
-

Project 1 and 2 instructions: see next page

Project 1 (specific instructions). 20% of term mark (plus **book content is in-scope for Midterm 2**)

This is a single-student independent technical report on *Permanent Record* by Edward Snowden, 2019. The hardcover book is 336 pages, so **students should begin 4-6 weeks before the due date**. You may begin immediately, as *no additional material will be necessary or given, beyond these instructions*.

Collaboration. Reports must be **written individually** without significant collaboration. Students may post questions for clarification on our Discord channel (which the TAs will monitor) and may discuss high-level aspects, but may not post or distribute any specific details in written, video or voice recordings, nor directly use specific notes from anyone else (your own personal notes from general discussions may be used); other sharing is viewed as **plagiarism** in this course. Re-read the **Academic Integrity** notes in the course outline.

Length and formatting. The report must **at least 5 full pages** of content (excluding references, if any), and **at most 6 full pages**. Other formatting instructions are as for all deliverables (see previous page).

Content. The report should summarize the book content most relevant to our course, especially on technical details and capabilities, discussion of metadata, societal impact, privacy, and surveillance. **Give page numbers** to locate the concepts you summarize, for example: *The author explains (p37) that metadata refers to...* Page numbers can be mid-sentence or at the end of sentences or paragraphs, and may include several pages (pp37-38) or (p37; p39; p86), but no ranges longer than 3 (instead, pick the 2 or 3 most relevant pages for a referenced item).

The report must begin with an **introductory paragraph** that explains what the report is about. If you also use an explicit abstract, do not repeat the abstract content in the opening paragraph.

You may provide your own insights and opinions, but if so, clearly explain and support them with convincing reasoning (justifying your lines of thought).

Figures and diagrams are not expected, but if you do use any, they must be of your own creation. Copy-and-paste of diagrams violates academic integrity in this course; also, *do not use screen captures*. If you redraw any diagrams, cite the source in a caption and explain (otherwise plagiarism issues arise).

Presentation appearance, grammar, clarity. It is expected that your report will have proper format and is free of errors in spelling, grammar, punctuation, etc. Reports failing to meet this expectation are **subject to a deduction of up to 20%** (4 marks) of the total available grade, independent of technical content; such failures typically also make the technical content unclear, further impacting the grade.

Additional guidance and suggestions:

- ❖ Make notes (e.g., pencil marks bracketing relevant sentences) **on your first reading pass** of the book. This may save a tremendous amount of time in finding relevant content for your report.
- ❖ **Provide context.** Your target reader should be typical 2nd-year CS students not in COMP2109.
- ❖ Make your report **self-contained**. Define any jargon used, i.e., any terminology that a typical 2nd-year CS student (peer student in courses outside of COMP2109) would not understand.
- ❖ **Formal references.** See the previous page for explicit details specifying required reference style. You may, e.g., cite references used to help explain background relevant to the book.

Grading rubric: 20 marks for content. See above regarding **deductions**.

- 10 marks: **selection and coverage** of content, complete with page numbers as explained above.
- 5 marks: **clear and accurate** summary of content, conveying a technical understanding.
- 5 marks: **overall quality**. Includes being **self-contained** with **context** suitable to target reader.

Project 2: see next page

Project 2 specific instructions, beyond common instructions on page 1 above. 14 marks, 14% of term mark.

You may begin immediately, as no additional material will be given beyond these instructions.

Project 2 is a technical survey on a topic from the suggested list, written **individually** (not group work).

The content should focus on technical details related to security and privacy aspects of our course.

This content should be based on a review of primary sources, which must be cited.

You may include personal insights/opinions, if supported convincingly (justify your lines of thought).

Length (excluding references): **at least 5 full pages, at most 6**. See formatting instructions on page 1.

Presentation appearance, grammar, clarity. Reports are expected to have proper format and be free of errors in spelling, grammar, and punctuation. Failing this expectation risks **deduction of up to 20% (3 marks)** of the available grade, independent of technical content.

Figures. Any figures or diagrams included must be created by you; use of copy-and-pasted diagrams violates academic integrity in this course. Avoid using *screen captures* unless they clearly add value (and in that case, explain their value; these also do not count towards the word-count of page content). For any redrawn diagrams, you must cite the source in a diagram caption.

Additional guidance and suggestions:

- ❖ Begin with an *introductory paragraph* clearly explaining what the report is about.
If you use an explicit abstract, do not duplicate the same content in the opening paragraph.
- ❖ *Provide context.* Your target reader should be typical second-year CS students not in COMP2109
- ❖ Make the report *self-contained*. Define any jargon or terminology that typical second-year CS students would not understand.
- ❖ *Include formal references.* See page 1 for explicit details specifying required reference style.
Cite your primary source references, and others that helped you explain background items.

Grading rubric: 14 marks for content. See above regarding *deductions*.

- 6 marks: **selection of content** and **coverage of details**, including **references** as noted above.
- 4 marks: **clear** and **accurate** summary of topic, conveying a technical understanding.
- 4 marks: **overall quality**, being **self-contained**, and **context** suitable to target reader.

List of topics. (Other topics may also be allowed; to request *special permission*, email the Instructor *before Mar 21, 2023*, providing details of the proposed topic and 2-4 primary sources you plan to use.)

1. **Passkeys & WebAuthn** (FIDO standards): methods to replace/improve on regular passwords.
2. **Smart contracts**: and their relationship to blockchain-based **non-fungible tokens** (NFTs).
3. **Tor**: technical details, its positive aspects, and its negative aspects in the real world.
4. **Mixmaster** (Type II remailer): its technical details, real world implementations, and use.
5. **Ad blockers**: how they work. (Alternative: mechanisms to avoid web user tracking.)
6. Privacy risks related to **information sharing on online social networks**, such as **Facebook**.
7. **Cambridge Analytica scandal**: technical details, privacy implications, or risks to democracies posed by exploiting personal profiles via social network data.
8. **Rust**: as a safe systems programming language alternative to C.
9. **Software fuzzing**: as a technology to improve software security testing.
10. **CVEs and CWEs**: technical details of what they are, and how they help the software industry.