Thesis Project Portfolio

Competitive Learning: Successes and Pitfalls from Two Years of the University of Virginia's High School Programming Contest

(Technical Report)

Cryptography and the Right to Privacy in the United States during the Emergence of the Internet

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Nicholas James Winschel

Spring, 2025

Department of Computer Science

Table of Contents

Sociotechnical Synthesis

Competitive Learning: Successes and Pitfalls from Two Years of the University of Virginia's High School Programming Contest

Cryptography and the Right to Privacy in the United States during the Emergence of the Internet

Prospectus

Executive Summary

The social implications of technologies are not completely decided by the details of technologies themselves–broader context is required to understand their impact. Computing, as a field, has seen explosive growth in the last half century. A recurring theme in computing technologies is the impact of *access*. Access broadly decides the social implications of computing technologies–it chooses ingroups and outgroups, modulates fairness of automated decision making, and selectively increases the communication potential of some at the expense of others. Efforts at improving outcomes with computing, especially in education, focus on improving access to existing computing technologies. For communication technologies, too, cryptography provides an interesting example of the impacts of access. Cryptography is the science and practice of securing information in communication and at rest. The recent history of cryptography is remarkable, as denial of access to cryptography is often overt, intentional, and frequently the subject of debate.

We undertook an effort to improve access to computing education by running a High School Programming Contest (HSPC) at the University of Virginia. A programming contest is a contest where students compete to solve a number of algorithmic problems from short specifications. These algorithmic problems usually consist of turning some desired input into some desired output, and can almost always be solved in less than 200 lines of code. Our programming contest had teams of three high schoolers competing to solve around ten of these problems in four and a half hours, with a single computer per team. The intended purpose of this contest is to teach students effective problem solving, time management, teamwork, and creativity in algorithm design. We ran this competition for two years (2023-2024), scaling it to more than 30 teams participating. As Head Judge, I oversaw the technical aspects of the

competition: judging infrastructure, competition environments, competition networking, typesetting, problem set construction, and test case generation. I had much help in implementing all of these, and I found tactics that helped me maximize effectiveness in all of these. We generally found students satisfied with the contest, but its true impact will likely not be seen for years to come.

Access to cryptography is in part determined by regulations governing allowed or required forms of encryption. There is a complex relationship between these regulations, development of cryptographic technologies, and the right to privacy as it pertains to these regulations. This interplay was especially visible during the emergence of the internet in the United States, as brand-new technology that enabled accessible, instantaneous communication emerged at roughly the same time as improved technology that allowed said communication to be performed secretly. Increasing use of both of these technologies contributed to changes in the notion of a "right to privacy" in the United States. This gives rise to a question: In the United States, how has the concept of "the right to privacy" shaped early cryptographic regulation, and to what extent has available cryptographic technology shaped the right to privacy? For the first part of this question, I claim that the right to privacy had a limited impact on early cryptographic regulation–it lost in contests with national security, and its constructive effects were achieved with the help of economic interests and appeals to freedom of speech. I reach this conclusion by analyzing the stated intents of several illustrative pieces of regulation. I answer the second part of the question by appealing to the "technological dramas" framework of Pfaffenberger, casting developments in cryptographic technology–and resulting use–as political statements and support for those statements, respectively. I argue that understanding these relationships is key to developing effective cryptographic policy.

These results together constitute some contribution to the field of “access in computing.” I am greatly satisfied with the lessons learned from running the HSPC–I was able to successfully apply lessons learned from the two years covered by the report to the 2025 iteration of the contest, and I expect the contest to be run well in the future as well. A possible point of future improvement would be the creation of a more robust system for assessing problem difficulty, as the current system is vague and creates inaccuracies. I am also satisfied with the results of the analysis of cryptographic regulations and the right to privacy. I found less of an impact in one direction than expected, but I do believe that my methods were useful. A possible point of future research would be applying the technological dramas framework to analyze international relations with regards to cryptography and surveillance, as my analysis was mostly domestic in nature. I believe that such an analysis would likely have to focus on a wider timeframe. In all, I hope that I have both improved access to computing and contributed some account of the impacts of access to computing, even if the domains were relatively far apart.