

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

**SAMSUNG ELECTRONICS CO., LTD. AND
SAMSUNG ELECTRONICS AMERICA, INC.,**
Petitioners

v.

MAXELL, LTD.,
Patent Owner

Inter Partes Review No.: IPR2024-00828

**DECLARATION OF SETH JAMES NIELSON, PH.D.,
IN SUPPORT OF PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 8,982,086**

I hereby declare that all statements made herein of my own knowledge are true, and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine and/or imprisonment under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the patent which is under review in this proceeding.

Date: April 26, 2024



Seth James Nielson, Ph.D.

TABLE OF CONTENTS

	Page
EXHIBITS	viii
I. Introduction.....	1
II. Background and Qualifications	1
III. Documents and Other Materials Relied Upon.....	9
IV. Statutory Grounds for Challenge	9
V. Relevant Patent Law and Legal Standards	10
A. Date of Invention.....	10
B. Anticipation	10
C. Obviousness.....	10
D. Standard of Proof.....	14
VI. Level of Ordinary Skill in the Art	14
VII. The '086 Patent and Its Prosecution Histories	15
A. Overview of the '086 Patent.....	15
B. Prosecution History	19
C. Reexamination of the '086 Patent	19
D. Reissue of U.S. Patent No. 8,654,093 (“RE48,830”).....	19
VIII. Claim Construction.....	20
B. “first information necessary for an identification of the user” (all claims).....	20
C. “second camera arranged on an opposite side of the touch display” / “second camera being arranged on an opposite side of the touch display” (claims 1, 11).....	21
IX. Overview of the Prior Art.....	22
A. Rogers (EX1006).....	22
B. Rosenberg (EX1007).....	28
C. Miyazawa (EX1008)	30

D.	Rekimoto (EX1010)	32
X.	Ground 1: The Combination of rogers and rosenberg Renders Challenged Claims 1, 2 and 4-7 Obvious	36
A.	Motivation to Combine Rogers with Rosenberg.....	36
B.	Claim 1	40
1.	[1pre] “An information processing apparatus comprising:”	40
2.	[1a] “a touch panel configured to detect a contact of a finger of a user;”	41
3.	[1b] “a detector configured to detect first information necessary for an identification of the user when the contact is detected between the touch panel and the finger of the user;”	43
4.	[1c] “a first controller configured to control the information processing apparatus to operate into two operating modes: at least an identification mode and a registering mode, as the operating mode thereof;”	45
5.	[1d] “memory that is configured to store second information relating to the identification of the user, which is stored in advance; and”	50
6.	[1e] “a second controller configured to execute a specified process when said first information and said second information are coincident within said identification mode, wherein:”	52
7.	[1f] “[] in said registering mode, there are provided a first registering mode for inputting input information by a pad of the finger, and a second registering mode for inputting input information by an end of the finger, and said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode.”	56
C.	Claim 2 “The information processing apparatus according to claim 1, wherein said first information includes a position and an area of the finger contacting with said touch panel.”	64

D.	Claim 4 “The information processing apparatus according to claim 1, wherein said specified process includes releasing of a lock of resting an operation of said information processing apparatus.”	65
E.	Claim 5 “The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display a first image and first descriptive text associated with the first registering mode and a second image and second descriptive text associated with the second registering mode.”	66
F.	Claim 6 “The information processing apparatus according to claim 1, wherein the touch panel includes one or more capacitive sensors, such that the contact of the finger is detected based on variations in capacitance of the one or more capacitive sensors in response to the contact.”	70
G.	Claim 7 “The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display information during the identification mode that informs the user to use a finger to execute an unlock operation of the information processing apparatus.”	72
XI.	Ground 2: The Combination of rogers, rosenberg, AND miyazawa Renders Challenged Claims 9-14 Obvious	73
A.	Motivation to Combine with Rosenberg and Miyazawa	73
B.	Claim 9 “The information processing apparatus according to claim 1, wherein the first controller is configured to execute one or more of tapping, dragging, flicking, and pinching operations based on the detection of contact of the finger.”	76
C.	Claim 10 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute tapping operations, and the tapping operations include detection of contact of the finger for a first time period.”	79
D.	Claim 11 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period.”	80

E.	Claim 12	82
1.	[12a] “The information processing apparatus according to claim 9, wherein the first controller is configured to execute flicking operations, and the flicking operations correspond to the user sliding the finger for a first time period, and”	82
2.	[12b] “wherein the first controller is configured to execute pinching operations, and the pinching operations correspond to the user establishing two contacts and increasing the distance between the established two contacts.”	84
F.	Claim 13	85
1.	[13a] The information processing apparatus according to claim 9, wherein the first controller is configured to execute said dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first tie period, and	85
2.	[13b] wherein the first controller is configured to execute said flicking operations, and the flicking operations correspond to the user sliding the finger for a second time period that is shorter than the first time period.	86
G.	Claim 14. The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen displaying a plurality of icons corresponding to applications being executed on the information processing apparatus, and the information processing apparatus is configured to execute an operation for moving at least one of the plurality of icons based on an operation that requires contact by a finger for a predetermined period of time.	87
XII.	Ground 3: The Combination of rogers and Rekimoto Renders Challenged Claims 1, 2 and 4-7 Obvious	90
A.	Motivation to Combine Rogers with Rekimoto	90
B.	Claim 1	94
1.	[1pre] An information processing apparatus comprising:	94

2. [1a] a touch panel configured to detect a contact of a finger of a user; 94
 3. [1b] a detector configured to detect first information necessary for an identification of the user when the contact is detected between the touch panel and the finger of the user; 94
 4. [1c] a first controller configured to control the information processing apparatus to operate into two operating modes: at least an identification mode and a registering mode, as the operating mode thereof; 94
 5. [1d] memory that is configured to store second information relating to the identification of the user, which is stored in advance; and 94
 6. [1e] a second controller configured to execute a specified process when said first information and said second information are coincident within said identification mode, wherein: 95
 7. [1f] in said registering mode, there are provided a first registering mode for inputting input information by a pad of the finger, and a second registering mode for inputting input information by an end of the finger, and said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode. 95
- C.** Claim 2. The information processing apparatus according to claim 1, wherein said first information includes a position and an area of the finger contacting with said touch panel. 99
- D.** Claim 4. The information processing apparatus according to claim 1, wherein said specified process includes releasing of a lock of resting an operation of said information processing apparatus. 99
- E.** Claim 5. The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display a first image and first descriptive text associated with the first registering mode and a second image

	and second descriptive text associated with the second registering mode.....	99
F.	Claim 6. The information processing apparatus according to claim 1, wherein the touch panel includes one or more capacitive sensors, such that the contact of the finger is detected based on variations in capacitance of the one or more capacitive sensors in response to the contact.	102
G.	Claim 7. The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display information during the identification mode that informs the user to use a finger to execute an unlock operation of the information processing apparatus.....	102
XIII.	Ground 4: The Combination of rogers, rekimoto AND miyazawa Renders Challenged Claims 9-14 Obvious.....	103
A.	Motivation to Combine Rogers with Rekimoto and Miyazawa	103
B.	Claim 9 “The information processing apparatus according to claim 1, wherein the first controller is configured to execute one or more of tapping, dragging, flicking, and pinching operations based on the detection of contact of the finger.”	105
C.	Claim 10 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute tapping operations, and the tapping operations include detection of contact of the finger for a first time period.”	106
D.	Claim 11 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period.”	106
E.	Claim 12	106
1.	[12a] “The information processing apparatus according to claim 9, wherein the first controller is configured to execute flicking operations, and the flicking operations correspond to the user sliding the finger for a first time period, and”	106

2.	[12b] “wherein the first controller is configured to execute pinching operations, and the pinching operations correspond to the user establishing two contacts and increasing the distance between the established two contacts.”	107
F.	Claim 13	107
1.	[13a] “The information processing apparatus according to claim 9, wherein the first controller is configured to execute said dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period, and”	107
2.	[13b] “wherein the first controller is configured to execute said flicking operations, and the flicking operations correspond to the user sliding the finger for a second time period that is shorter than the first time period.”	107
G.	Claim 14. “The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen displaying a plurality of icons corresponding to applications being executed on the information processing apparatus, and the information processing apparatus is configured to execute an operation for moving at least one of the plurality of icons based on an operation that requires contact by a finger for a predetermined period of time.”	107
XIV.	Conclusion	108

EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 8,982,086
1002	File History of U.S. Pat. 8,982,086
1003	Declaration of Seth James Nielson, Ph.D.
1004	Reexamination File History of U.S. Patent No. 8,982,086
1005	Reissue File History of U.S. Patent No. 8,654,093
1006	U.S. Patent No. 8,683,582 (“Rogers”)
1007	U.S. Patent Publication No. 2007/0097096 (“Rosenberg”)
1008	U.S. Patent No. 8,633,909 (“Miyazawa”)
1009	U.S. Patent No. 7,877,707 (“Westerman”)
1010	U.S. Patent No. 8,477,115 (“Rekimoto”)
1011	U.S. Patent No. RE48,830 (“RE48,830”)

TABLE OF CLAIMS

[1pre] An information processing apparatus comprising:
[1a] a touch panel configured to detect a contact of a finger of a user;
[1b] a detector configured to detect first information necessary for an identification of the user when the contact is detected between the touch panel and the finger of the user;
[1c] a first controller configured to control the information processing apparatus to operate into two operating modes: at least an identification mode and a registering mode, as the operating mode thereof;
[1d] memory that is configured to store second information relating to the identification of the user, which is stored in advance; and
[1e] a second controller configured to execute a specified process when said first information and said second information are coincident within said identification mode, wherein:
[1f] in said registering mode, there are provided a first registering mode for inputting input information by a pad of the finger, and a second registering mode for inputting input information by an end of the finger, and said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode.
[2] The information processing apparatus according to claim 1, wherein said first information includes a position and an area of the finger contacting with said touch panel.
[4] The information processing apparatus according to claim 1, wherein said specified process includes releasing of a lock of resting an operation of said information processing apparatus.
[5] The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display a first image and first descriptive text associated with the first registering mode and a second image and second descriptive text associated with the second registering mode.

[6] The information processing apparatus according to claim 1, wherein the touch panel includes one or more capacitive sensors, such that the contact of the finger is detected based on variations in capacitance of the one or more capacitive sensors in response to the contact.

[7] The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display information during the identification mode that informs the user to use a finger to execute an unlock operation of the information processing apparatus.

[9] The information processing apparatus according to claim 1, wherein the first controller is configured to execute one or more of tapping, dragging, flicking, and pinching operations based on the detection of contact of the finger.

[10] The information processing apparatus according to claim 9, wherein the first controller is configured to execute tapping operations, and the tapping operations include detection of contact of the finger for a first time period.

[11] The information processing apparatus according to claim 9, wherein the first controller is configured to execute dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period.

[12a] The information processing apparatus according to claim 9, wherein the first controller is configured to execute flicking operations, and the flicking operations correspond to the user sliding the finger for a first time period, and

[12b] wherein the first controller is configured to execute pinching operations, and the pinching operations correspond to the user establishing two contacts and increasing the distance between the established two contacts.

[13a] The information processing apparatus according to claim 9, wherein the first controller is configured to execute said dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period, and

[13b] wherein the first controller is configured to execute said flicking operations, and the flicking operations correspond to the user sliding the finger for a second time period that is shorter than the first time period.

[14] The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen displaying a plurality of icons corresponding to applications being executed on the information processing apparatus, and the information processing apparatus is configured to execute an operation for moving at least one of the plurality of icons based on an operation that requires contact by a finger for a predetermined period of time.

I. INTRODUCTION

I, Seth James Nielson, Ph.D., declare as follows:

1. My name is Seth James Nielson. I have been asked by Petitioners Samsung Electronics Co. Ltd. and Samsung Electronics America, Inc. to provide my expert opinions in support of the above-identified petition for *inter partes* review of U.S. Patent No. 8,982,086 (“’086 patent,” EX1001), challenging the validity of claims 1, 2, 4-7, and 9-14 (the “Challenged Claims”).

2. I currently hold the opinions set forth in this declaration.

3. In summary, it is my opinion that the references cited below render obvious the Challenged Claims. My detailed opinions on the claims are set forth below.

4. I am being compensated for my time at the rate of \$700 per hour. This compensation is not contingent upon my performance, the outcome of this matter, or any issues involved in or related to this matter.

II. BACKGROUND AND QUALIFICATIONS

5. I am a subject matter expert in cybersecurity, computer networks, and software engineering. I have been working as a computer scientist professionally for over twenty years including projects in industry, academia, government, and non-profits. In terms of education, I received my B.S. in Computer Science from Brigham Young University (BYU) in April of 2000. I subsequently received my

M.S. in Computer Science from BYU in August of 2004. Later, I earned my Ph.D. in Computer Science from Rice University in December 2009.

6. Currently, I am the Founder and Chief Scientist of Crimson Vista, a computer security research and engineering company. I started Crimson Vista in March 2016. Prior to that, I worked as a Software Engineer at Quallaby in 2000, Lineo/Metrowerks from 2001-2003, and Google in the summer of 2005. I worked in technical consulting form 2005-2011 at Independent Security Evaluators and at Harbor Labs from 2011-2015.

7. Furthermore, I currently hold appointments at the University of Texas at Austin as an Adjunct Associate Professor in the department of Computer Science and as a Cybersecurity Fellow in the Robert Strauss Center for International Security and Law. I previously held appointments as an Adjunct Research Scientist in the Computer Science department of the Johns Hopkins University from 2014-2019. From 2016-2019 I was also the Director of Advanced Research Projects in the Information Security Institute.

8. I am also the co-founder of the nonprofit Crypto Done Right foundation.

9. During my work as a software engineer at Quallaby, Metrowerks, and Google, I created, tested, and/or maintained hundreds of thousands of lines of source code in a wide range of computer programming languages. This included

components related to computer networking, graphical user interfaces (GUIs), operating system build/configuration, web communications, automated deployment of software, virtual machines, and secure communications.

10. Moreover, while consulting at Independent Security Evaluators (ISE), I was also the technical lead for the development of software for a client. I designed and managed the implementation of the system, which involved improved communication systems for secure channels on the Internet. This system provided new benefits for distributing trust in Certificate Authorities, which are often the weak link in TLS security.

11. At ISE, I worked on a wide range of development projects for clients related to security features. These projects included a software encryption library, including the necessary tests and procedures for Federal Information Processing Standards (“FIPS”) certification. The encryption library also provided advanced operations such as secure data splitting and recovery. I also developed a parallel-program for massive code coverage analysis, GPU hardware-accelerated AES encryption, and distributed (encrypted) file-system prototypes.

12. In my work as a cybersecurity analyst at ISE, Harbor Labs, and Crimson Vista, I have performed security evaluation services that included port-scanning analyses, security protocol analysis using formal and exploratory methods, and security breach investigations. Clients include large banks, major

medical device manufacturers, The MPAA and RIAA jointly, hospitals, cyber-insurance companies, start-up companies, media companies, and financial institutions. My analyses include reviews of programming code (e.g., for bugs/vulnerabilities), cryptography, and forensics.

13. As a security expert, I offered services broadly within the scope of “security engineering.” This holistic process provides comprehensive analysis, design, and insight into cybersecurity concerns before, during, and after development. A key component of my approach to security engineering includes data discovery, architecture, and quality control as a critical first-step in security (i.e., “you can’t secure data you don’t know about”). I have applied these models to various clients including clients for whom I have provided contract Chief Information Security Officer (CISO) services.

14. I have also provided technical guidance to an antitrust team in the United States Department of Justice. Although the technologies and parties are confidential, I can disclose that I provided in-person training on technical topics and analyses of competing security products.

15. My expertise in cryptography has also led me to consult on a number of projects related to blockchain and distributed ledgers. I have consulted on issues related to smart contracts, use-cases for distributed ledger functionality, and deployment considerations.

16. In addition to consulting with companies, I have also provided training on security, privacy, and blockchain at the Data Architecture Summit and Enterprise Data World conferences.

17. Another area of expertise is forensic analysis including analysis of source code. For over a decade, at Harbor Labs and Crimson Vista, I have performed a wide range of code reviews for diverse technologies including CAD software, video game systems, digital mobile radios (DMRs), video streaming, networking, cryptography, antivirus, and digital rights management (DRM). I have been instrumental in multiple cases to discovering and identifying stolen or misappropriated source code. I have also investigated accusations of digitally tampered documents, sabotaged computer servers, and the provenance of digital assets. As Crimson Vista has grown, I have also directed teams of associates in security, forensic, and research efforts.

18. Beyond my work as an engineer and technical consultant, I have been involved in academic teaching, development, and research since my undergraduate degree. I first engaged in research in the Fall of 2000 on a project in the BYU computer science department related to networks and network resource management. Our work was published in the research paper “Effective Bandwidth for Traffic Engineering.”

19. During my Master's Degree in Computer Science, I conducted research in software engineering topics, with a special emphasis on how programmers think while creating and modifying code. My research included a study of software architectural patterns and their evolution over time. My research was published as "Design Dysphasia and the Pattern Maintenance Cycle," in the Journal Information and Software Technology August 2006. My thesis, which I completed in 2004, was largely based on this research.

20. During my Ph.D. work at Rice University, I conducted research into multiple topics including computer vulnerabilities and distributed computer security. In my research, I identified a security vulnerability in a Google product that existed at the time (Google Desktop Search). After contacting Google and assisting them in closing the vulnerability, we published the details of our investigation. I also published various papers including "A Taxonomy of Rational Attacks." My thesis, entitled "Designing Incentives for Peer-to-Peer Systems," was defended in late 2009.

21. I began teaching as an adjunct professor in 2014 at the Johns Hopkins University. I taught undergraduate and graduate studies in computer security. In 2016, the Information Security Institute appointed me as the Director of Advanced Research Projects. I collaborated with companies, government agencies, and other academic institutions to develop the research programs of the Information Security

Institute. I also mentored student capstone projects related to cryptography, drone security, iOS security, BitCoin, SSL vulnerabilities, and Twitter “botnets.” My students and I have published multiple papers from these capstone projects, including published research on cracking a portable chemical manufacturing system.

22. I began teaching at the University of Texas (“UT”) at Austin as an adjunct professor in 2019. I taught the undergraduate computer security class in the computer science department. I currently teach a special class on cybersecurity technology in the UT law school.

23. In all of these classes, I have developed my own curriculum. I created an experimental set of projects at the Johns Hopkins University about which I subsequently published a paper in the Journal of Computer Science Education entitled, “PLAYGROUND: Preparing Students for the Cyber Battleground.”

24. I also continue research at Crimson Vista. I was the primary investigator on a government funded research project. The project dealt with automatic recovery from ransomware attacks and was funded by the United States Army. The project was collaborative with academia, and I led a team of student researchers from Johns Hopkins and Brigham Young University in developing my design and implementing a prototype.

25. I am also a contributor to another small-business research project begun by a former student and funded by the National Science Foundation. We are researching the development of a new system for secure data storage that is protected even against “insider” threats, such as a rogue IT administrator.

26. I also gave a talk on “Detecting Malicious Sandboxes” at the Workshop on Defensive Deception and Trust in Autonomy, in association with the 2018 Naval Applications of Machine Learning Workshop.

27. I am also the co-founder and current director of the Crypto Done Right project. This project is originally hosted by Johns Hopkins University and funded by a grant from Cisco. I have transitioned the project into independent non-profit entity. Crypto Done Right is designed to bridge the gap between cryptography SME’s and the IT professionals that use it. It provides authoritative guidance on deployment, lifecycle, and management of cryptography in IT systems, software development, and technical management.

28. Finally, I am the author of “Cryptography in Python: Learning Correct Cryptography by Example.” I am also the author of the book “Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner,” which I use as my textbook for my students at UT.

29. My qualifications, publications, professional experience and expertise are set forth more fully in my curriculum vitae, attached as **Exhibit A**.

III. DOCUMENTS AND OTHER MATERIALS RELIED UPON

30. In forming the opinions set forth in this declaration, I have reviewed the documents in the following table:

Exhibit No.	Description
1001	U.S. Patent No. 8,982,086
1002	File History of U.S. Pat. 8,982,086
1004	Reexamination File History of U.S. Patent No. 8,982,086
1005	Reissue File History of U.S. Patent No. 8,654,093
1006	U.S. Patent No. 8,683,582 (“Rogers”)
1007	U.S. Patent Publication No. 2007/0097096 (“Rosenberg”)
1008	U.S. Patent No. 8,633,909 (“Miyazawa”)
1009	U.S. Patent No. 7,877,707 (“Westerman”)
1010	U.S. Patent No. 8,477,115 (“Rekimoto”)
1011	U.S. Patent No. RE48,830 (“RE48,830”)

31. Additionally, I have utilized my own experience and expertise, including regarding the knowledge and capabilities of a person of ordinary skill in the relevant art in the timeframe of the claimed priority date of the '086 patent.

IV. STATUTORY GROUNDS FOR CHALLENGE

32. In this declaration, I offer opinions on the following grounds that are the basis for this IPR proceeding:

Ground	Claims	Basis	Reference(s)
1	1, 2, 4-7	§103	Rogers, Rosenberg
2	9-14	§103	Rogers, Rosenberg, Miyazawa
3	1, 2, 4-7	§103	Rogers, Rekimoto
4	9-14	§103	Rogers, Rekimoto, Miyazawa

V. RELEVANT PATENT LAW AND LEGAL STANDARDS

A. Date of Invention

33. I have been asked to use the date of the filing of the earliest application to which priority is claimed (*i.e.*, February 9, 2011) as the date of invention for purposes of my analysis.

B. Anticipation

34. I am informed and understand that a patent claim is invalid under 35 U.S.C. §102 if a prior art disclosure teaches every element required by the claim, either expressly or inherently. The identical invention must be shown in as complete detail as is contained in the claim. When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art.

C. Obviousness

35. I am informed and understand that a patent claim is invalid under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention

to a person having ordinary skill in the art to which the subject matter pertains.

Obviousness, as has been explained to me, is based on (i) the scope and content of the prior art, (ii) the differences between the prior art and the claim, (iii) the level of ordinary skill in the art, and (iv) any secondary indicia of non-obviousness (*e.g.*, “secondary considerations” such as commercial success in the market place of the claimed invention), to the extent that they exist.

36. I further understand that obviousness may be demonstrated by showing that it would have been obvious to combine the teachings of more than one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of a person having ordinary skill in the art, the following are examples of approaches and rationales that may be considered:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of one known element for another to obtain predictable results;
- Use of a known technique to improve similar devices (methods, or products) in the same way;
- Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;

- Applying a technique or approach that would have been obvious to try (choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to a person having ordinary skill in the art; and
- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

37. I further understand that an invention may be obvious if one of ordinary skill in the art, facing a wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it may be obvious to a person of ordinary skill to try the known options. If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it

would improve similar devices in the same way, using the technique would have been obvious.

38. I further understand that a person of ordinary skill in the art is a hypothetical person who is presumed to be aware of all of the relevant art at the time of the invention. The person of ordinary skill may be able to fit together the teachings of multiple patents and/or printed publications employing ordinary creativity and the common sense that familiar items may have uses in another context or beyond their primary purposes.

39. I also understand that when considering the obviousness of a patent claim, one should consider whether a teaching, suggestion, or motivation to combine the references exists so as to avoid impermissibly applying hindsight when combining or modifying the prior art. I understand this test should not be applied rigidly, but that the test can be important to avoid such hindsight.

40. I also understand that one of ordinary skill in the art must have a reasonable expectation of success in combining or modifying prior art references.

41. I also understand that all elements of a claim must be considered in an obviousness analysis.

D. Standard of Proof

42. I understand that the standard to prove unpatentability in an *inter partes* review proceeding is by a preponderance of the evidence, which means more likely than not.

VI. LEVEL OF ORDINARY SKILL IN THE ART

43. I have considered the level of ordinary skill in the art relevant to the '086 patent. I understand that factors such as the education level of those working in the field, the sophistication of the technology, the types of problems encountered in the art, the prior art solutions to those problems, and the speed at which innovations are made may help establish the level of skill in the art.

44. After reviewing the '086 patent, the relevant portions of the prosecution history of the '086 patent, and cited references, it is my opinion that the field of art pertinent to the subject matter of the '086 patent is computing and mobile devices with touch interfaces and touch surface technology as well as the biometrics and user authentication functions of those devices.

45. Based upon my knowledge of this field, I conclude that a person of ordinary skill in the art ("POSITA") at the time the first priority application to the '086 patent was filed (on or around February 9, 2011) would have at least a Bachelor's Degree in electrical engineering, computer engineering, computer science, or a related field, with at least one to two years of experience in the field

of computing devices with touch interfaces. Additional education or experience might substitute for the above requirements.

46. At the time the first priority application to the to the '086 patent was filed (on or around February 9, 2011), I would have exceeded the qualifications of a POSITA under the definition above. By this time in 2011, I had B.S., M.S., and PhD degrees in computer science, and over 10 years of experience in computer science topics including image processing, software development, graphical user interfaces, and computer security. The opinions expressed in this declaration would not change if the level of experience varied by a few years.

VII. THE '086 PATENT AND ITS PROSECUTION HISTORIES

A. Overview of the '086 Patent

47. The '086 patent is directed to an apparatus having a touch panel that “displays a plurality of pieces of identification information including letters, figures, and symbols” that a user may select to identify him/herself. EX1001, 1:40-44. The '086 patent discloses the ability of the touch panel to distinguish between touches from a fingertip (also referred to as “finger tip input”) and touches from a finger pad (“finger pad input”). EX1001, 3:46-56, 5:20-42, 6:1-8, and FIGS. 3, 4A-6, 8-14.

FIG. 4A

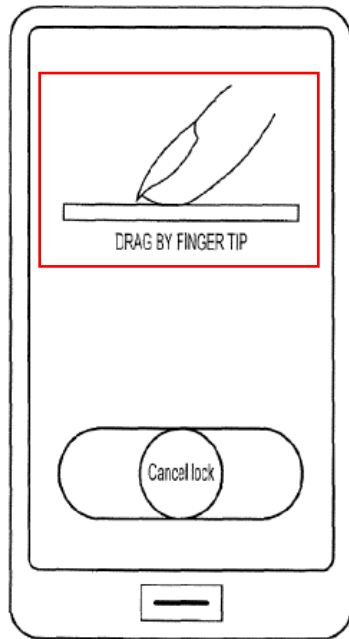
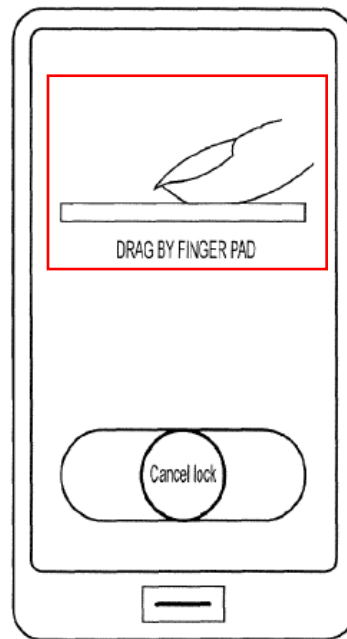


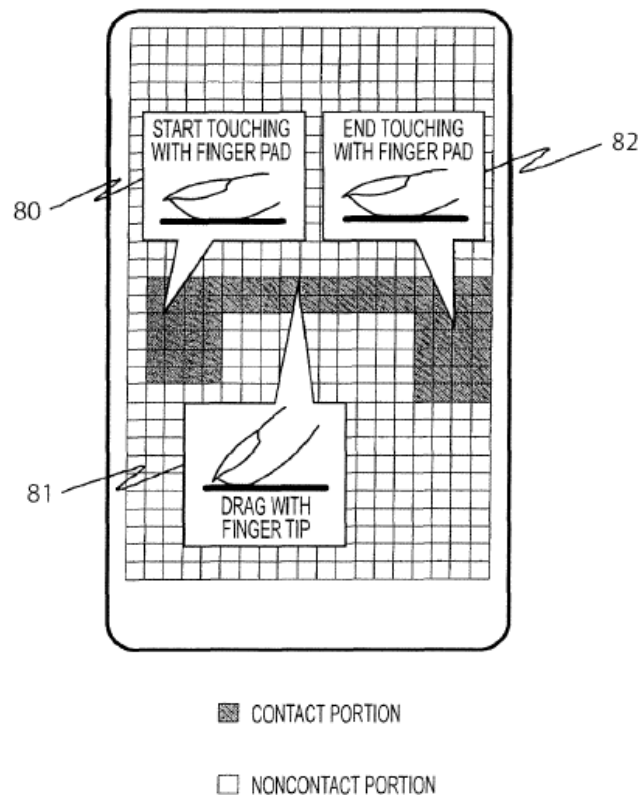
FIG. 4B



EX1001, FIGS. 4A, 4B.¹

¹ All emphasis, color, and annotations are added, unless otherwise indicated.

FIG. 8



EX1001, FIG. 8.

48. The “input using one’s finger pad is characterized in that the contact range of the finger and the touch panel 1 is wider than that of the fingertip input.” EX1001, 3:1-13. The ’086 patent also teaches associating the type of touch—fingertip versus finger pad—with the selected pieces of identification information to form a password for unlocking the device, thereby forming a password based on numbers, letters, symbols, etc. and the correct type of touch. EX1001, 6:12-7:63, and FIGS. 11-14. FIGS. 11A-11C and 12A illustrate a password formed from a combination of touch-type and numeric values. EX1001, 2:40-47, 2:48-49, 6:12-

7:63. Upon registering the password, the user presumably would subsequently unlock the device by entering the same sequence of numbers (“0528”) using the same sequence of touches (tip, pad, pad, pad).

FIG. 11A

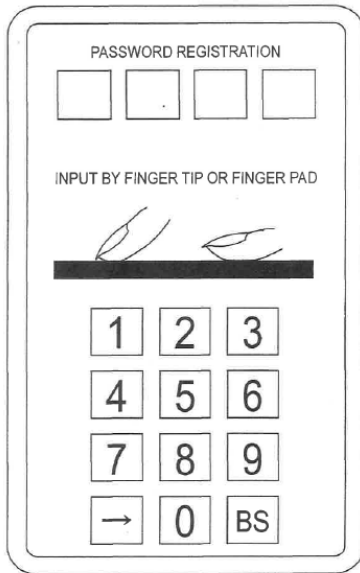


FIG. 12A

DIGIT	1	2	3	4
PASSWORD	0	5	2	8
INPUT METHOD	FINGER TIP	FINGER PAD	FINGER PAD	FINGER PAD

EX1001, FIGS. 11A, 12A.

49. The '086 patent also teaches different touch operations performed by the user, including “tapping, dragging, flicking, and pinching.” EX1001, 3:46-56. The control unit disclosed in the '086 patent distinguishes between the various disclosed touch operations by comparing the number of sensors that respond to the user’s touch while the operation is executed. EX1001, 5:20-42.

B. Prosecution History

50. U.S. Application no. 14/154,993 (“’993 application”), the application that issued as the ’086 patent, was filed on January 14, 2014, claiming priority to JP Application no. 2011-025576, filed on February 9, 2011. EX1001 (22), (30); EX1002, 172 (ADS). It is my understanding that for this IPR the Petitioners are not challenging whether the ’086 patent is entitled to the February 9, 2011 priority date or any priority date before the January 14, 2014 filing date.

51. The ’086 patent is also a continuation of U.S. Patent No. 8,654,093 (“’093 patent”), EX1001, (63), and issued with claims 1-4. EX1001, cols. 8-9.

C. Reexamination of the ’086 Patent

52. The ’086 patent was reexamined by the PTO as Reexamination Request No. 90/014,638, which resulted in a Reexamination Certificate issued on September 28, 2021. EX1004, 3-4 (Reexamination Certificate). The reexamination added claims 5-15. EX1004, 4 (Reexamination Certificate, p. 2).

D. Reissue of U.S. Patent No. 8,654,093 (“RE48,830”)

53. Patent Owner submitted the ’093 patent, the parent of the ’086 patent, for reissue on January 29, 2019. EX1005, 802. During that proceeding, Patent Owner attempted to add claims 8-34 that recited a memory for storing “first information corresponding to a fingerprint of the user.” EX1005, 622-629, 876-881. The Examiner rejected these claims for, among other things, lack of adequate written description support in the ’093 patent, which has the same specification as

the '086 patent. EX1005, 561 (“[t]here is no support for storing information related to a fingerprint, as the specification discloses storing information as to the fingertip or finger pad.”). The Examiner also rejected proposed claims 8-34 “as being based upon new matter added to the patent for which reissue is sought;” the Examiner cited the written description rejection as the basis for this position. EX1005, 562. Ultimately, Patent Owner canceled claims 8-34, and the application issued as RE48,830. EX1005, 1, 513-515, 539-541. The term “fingerprint” does not appear in any claim of RE48,830. EX1011, 8:50-10:58.

VIII. CLAIM CONSTRUCTION

54. In this section I list terms that require construction, and I have applied those constructions in my subsequent analysis. For all other terms, I applied the plain and ordinary meaning that a POSITA would have for the terms.

B. “first information necessary for an identification of the user” (all claims)

55. Claim 1 recites “first information necessary for an identification of the user.” Element [1b].

56. Petitioners propose this term to mean “information sufficient for the identification of the user, but not including information about a user’s fingerprint.”

57. It is my understanding from counsel that the doctrine of prosecution disclaimer prevents Patent Owner from trying to capture subject matter in its claims that the applicant explicitly conceded was not claimed.

58. In this instance, during prosecution of RE48,830, Patent Owner tried to claim “information corresponding to a fingerprint of the user” in an attempt to contend that “fingerprint information” was a type of user “information.” EX1005, 622-629, 876-881. The Patent Office rejected that effort, concluding that the patent’s written description would not support it. EX1005, 561. Patent Owner thereafter cancelled those claims, confirming that the claimed “information” cannot include “fingerprint” information. EX1005, 513-515, 539-541. Petitioners’ construction properly reflects PO’s disclaimer of claim scope.

59. It is my understanding that Petitioners propose this construction to be consistent with their proposed construction in the concurrent litigation. In my opinion, however, the Board need not rule on this construction because the prior art cited herein, and upon which I have based my opinions, discloses the components for detecting, storing and/or using the “first information necessary for an identification of the user” whether it can/cannot include “information about a user’s fingerprint.”

C. “second information relating to the identification of the user” (all claims)

60. Claim 1 recites “second information relating to the identification of the user.” Element [1f].

61. Petitioners propose this term to mean “information related to the identification of a user, but not including information about a user’s fingerprint.”

62. It is my understanding from counsel that the doctrine of prosecution disclaimer discussed for Petitioners' construction of "first information" applies to this term also. For the same reasons discussed above with respect to that term, Patent Owner clearly disclaimed information about a user's fingerprint, and the construction of "second information relating to the identification of the user" must also reflect that disclaimer.

63. It is my understanding that Petitioners also propose this construction to be consistent with their proposed construction in the concurrent litigation. In my opinion, however, the Board need not rule on this construction because the prior art cited herein, and upon which I have based my opinions, discloses the components for detecting, storing and/or using the "second information relating to the identification of the user" whether it can/cannot include "information about a user's fingerprint."

IX. OVERVIEW OF THE PRIOR ART

A. Rogers (EX1006)

64. U.S. Patent No. 8,683,582 ("Rogers") was filed on June 16, 2008 and issued March 25, 2014. I am informed that Rogers is prior art to the '086 patent under 35 U.S.C. §102(e).

65. Rogers is directed to a method and system for using graphical passcodes on touch sensitive electronic devices. EX1006, Abstract. Rogers

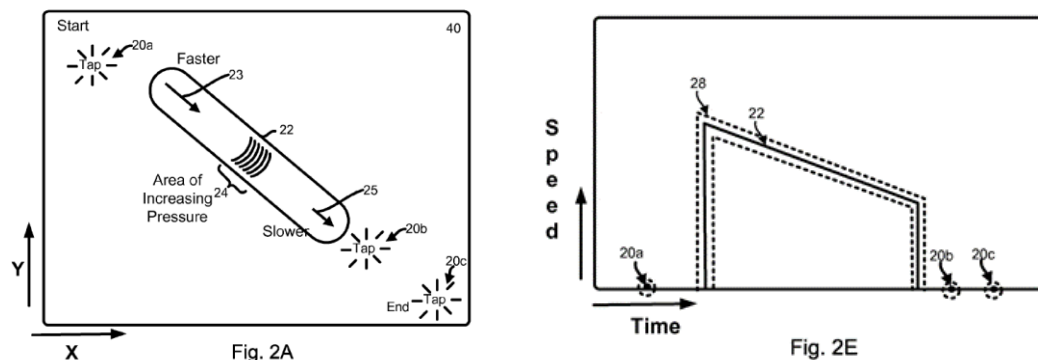
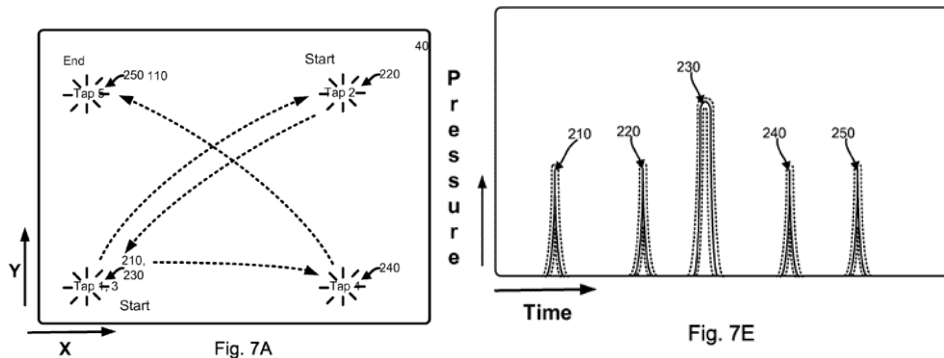
explains that “[g]raphical passcodes comprise various combinations of swipes, taps or drags on a touchscreen surface as defined by a user.” EX1006, Abstract.

Graphical passcodes are used “in the same manner that conventional passwords, security codes or personal identifiers are currently used.” EX1006,3:14-16. A user’s “graphical passcode is stored in memory for comparison to subsequent entries of [a] graphical passcode in order to authenticate users.” EX1006, Abstract. The graphical passcodes “can be used to lock or unlock an electronic device, provide or deny access to specific files or documents, operate a mechanical lock or vehicle, or identify an individual to an electronic device, network, or website.” EX1006, 13:16-20. The graphical passcode can also be translated by an “application development platform” that “may translate the coded signal to a useful input of any number of programs.” EX1006, 14:2-14.

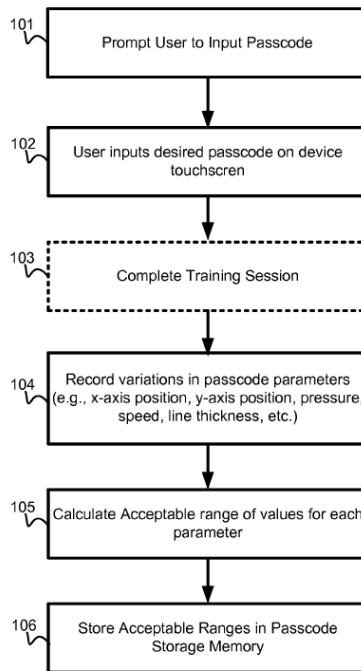
66. Rogers explains that graphical passcode is “a figure, drawings, letter, or shape input on a touchsurface such as by a user’s finger or a stylus.” EX1006, 3:32-34. The graphical passcode is “a series of touches, swipes, and/or taps on a touchsurface of varying pressure, speed and position.” EX1006, 3:34-36. The user “creates [this] graphical passcode by touching a touchsurface in a series of movements and touches within a brief period of time.” EX1006, 3:60-62.

67. When a user is registering a graphical passcode, measurable parameters, such as “timing speed, pressure, force, line thickness, contact area, or

location,” can be measured. EX1006, 4:15-21. The measured parameters can then be correlated to positional coordinates on the touchscreen and stored as a part of the template graphical passcode. EX1006, 4:21-27; *see also, e.g.*, EX1006, 10:40-49 (explaining that Figs. 7A and 7E (reproduced below) depict an “exemplary graphical passcode . . . consist[ing] of five taps 210, 220, 230, 240, and 250” and the “plot of pressure versus time” for those five taps, respectively); EX1006, 5:49-52, 6:14-15 (stating that Figs. 2A and 2E (reproduced below) show “an exemplary graphical passcode consisting of a tap, a swipe, and two taps” and “the plot of speed versus time for the passcode of Fig. 2A”, respectively).

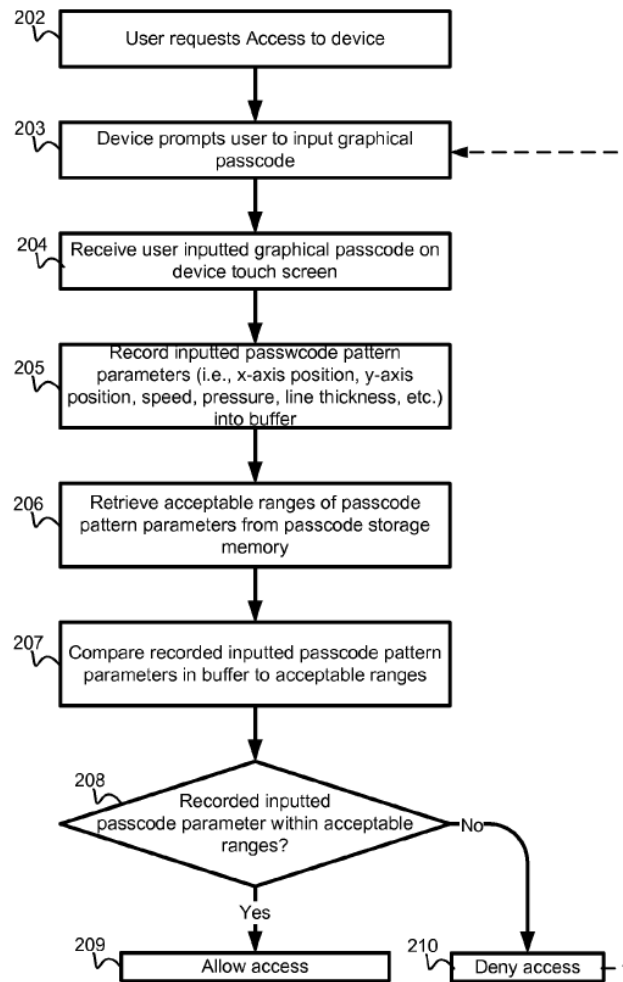


68. Rogers describes a first mode of operation for the registration or creation and storage of a user's graphical passcode in FIG.4 and the accompanying text at 8:41-9:28.



EX1006, FIG. 4.

69. Rogers describes a second mode of operation for using the registered graphical passcode to unlock an electronic device in FIG.5 and the accompanying text at 9:29-10:3.



EX1006, Fig. 5.

70. Rogers also teaches that the various disclosed embodiments “may be implemented with a variety of touch screen or touchpad technologies, including . . . capacitive touch screens.” EX1006, 1:66-2:2. Indeed, “[i]n some embodiments, a touchsurface can be provided in areas of the electronic device 70 outside of the touchscreen 40. For example, the keypad 76 can include a touchsurface with buried capacitive sensors.” EX1006, 5:28-31; *see also* FIG. 1 (showing a touch

screen, 40, which may be capacitive) (reproduced below), FIG. 13 (showing a touch screen, 40, which may be capacitive) (reproduced below).

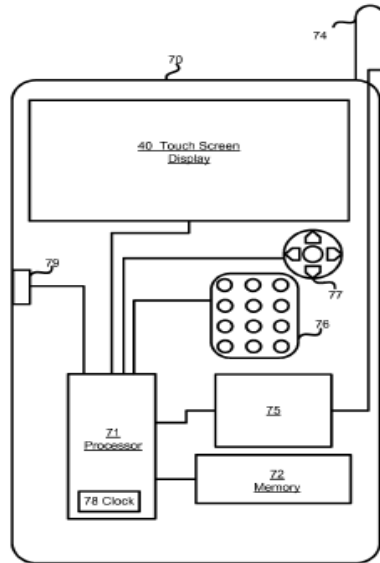


Fig. 1

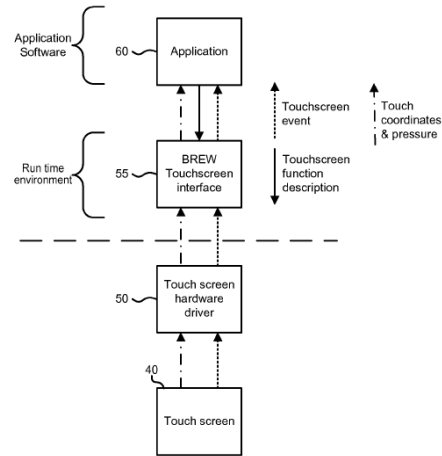


Fig. 13

71. Rogers further discloses embodiments that “include a capacitive touch screen which is coated with a material that conducts a continuous electrical current across the sensor. When the sensor’s ‘normal’ capacitance field (its reference state) is altered by another capacitance field, *i.e.*, someone’s finger, electronic circuits located at each corner of the panel measure the resultant ‘distortion’ in the sine wave characteristics of the reference field and send the information about the event to the controller for mathematical processing.” EX1006, 13:51-59.

B. Rosenberg (EX1007)

72. U.S. Patent Publication No. 2007/0097096 (“Rosenberg”) was filed on January 23, 2007 and published May 3, 2007. I am informed that Rosenberg is prior art to the ’086 patent under 35 U.S.C. §§102(a), 102(b).

73. Rosenberg discloses inputting input information by a pad of the finger (“pad-pointing”) and inputting input information by an end of the finger (“tip-pointing”): “embodiments of the present invention are operative to distinguish between finger-tip interactions (referred to herein as “tip-pointing”) where the user engages the touch screen with the tip of his or her finger and finger-pad interactions (referred to herein as “pad-pointing”) where the user engages the touch screen with the pad of his or her finger.” EX1007, ¶30. According to Rosenberg, “a variety of methods for distinguishing between finger-tip interactions and finger-pad interactions, including an assessment of the finger contact area size, shape, and/or orientation” are used to “enable mode selection in a particularly natural and intuitive manner, based upon the orientation in which the user’s finger engages the touch screen.” EX1007, ¶¶27, 28, 45.

74. Rosenberg explicitly discloses distinguishing between pad-pointing as opposed to tip-pointing “[b]ased upon the size and/or shape” of the contact area (shown as an ellipse A’ in FIG. 6):

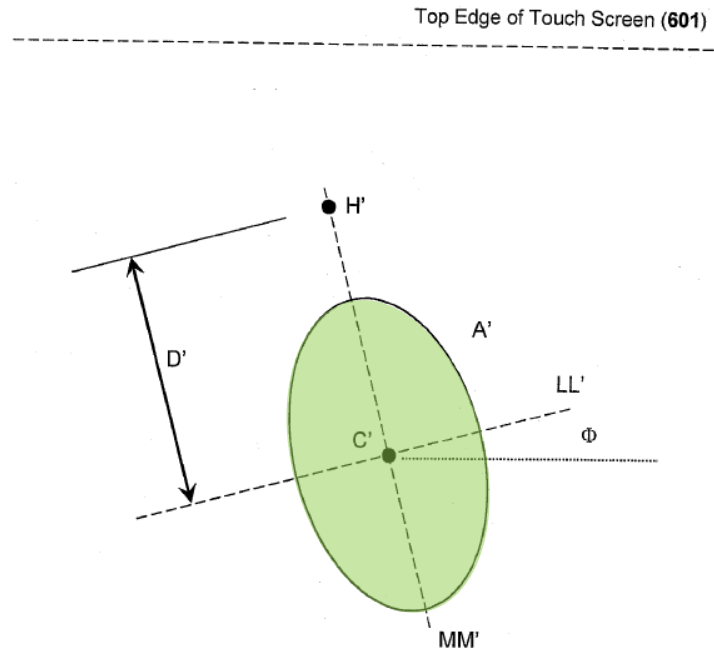


Fig. 6

EX1007, FIG. 6.

75. Rosenberg provides an example in which pad-pointing is shown in FIG. 8A and tip-pointing is shown in FIG. 8B. EX1007, ¶50.

Fig 8a

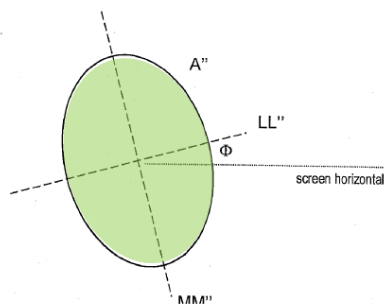
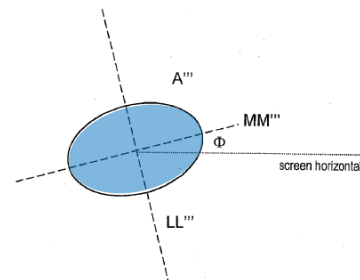


Fig 8b



76. The tip-pointing interaction (FIG. 8B) “is substantially smaller in size (both area and circumference), more eccentric in shape (i.e., less rounded), and is oriented such that the major axis MM''' is oriented closer to the reference screen

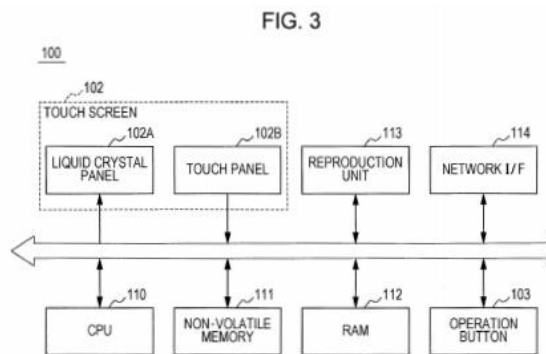
horizontal.” EX1007, ¶50. The pad-pointing interaction (FIG. 8A) “is substantially larger in size (both area and circumference), is less eccentric in shape (i.e., more rounded), and is oriented such that the minor axis LL" is oriented closer to the reference screen horizontal.” EX1007, ¶50. “Thus, each of the size, shape, and/or orientation of the detected finger contact area may be used alone or in combination by the routines of the present invention to distinguish between a tip-pointing interaction and a pad-pointing interaction.” EX1007, ¶50.

C. Miyazawa (EX1008)

77. U.S. Patent No. 8,633,909 (“Miyazawa”) was filed on December 29, 2010 and issued January 21, 2014. I am informed that Miyazawa is prior art to the ’086 patent under 35 U.S.C. §102(e)

78. Miyazawa discloses “[a]n information processing apparatus” that “includes: a touch detection unit detecting touch of an instruction object on an operation surface; a proximity detection unit detecting proximity of the instruction object to the operation surface; and a control unit determining whether the touch of the instruction object is a predetermined input operation based on the detection result, which is obtained by the touch detection unit when the touch detection unit detects the touch of the instruction object, and at least one of the detection results, which are obtained by the proximity detection unit before and after the touch of the instruction object.” EX1008, Abstract.

79. The information processing apparatus disclosed in Miyazawa recognizes various user touch operations, or gestures, based on the detection of positions on the touch panel touched with an instruction object. EX1008, 1:46-51; *see also* FIG. 3 (showing the controller (CPU 110) configured to execute the claimed operations based on the detection of contact of the finger with touch panel 102B):



80. “[T]he hardware configuration of the portable terminal 100 will be described with reference to FIG. 3. In the portable terminal 100, a CPU 110 develops a program stored in a non-volatile memory 111 into a RAM 112 and reads the program to perform various processes according to this program and control each unit. A central processing unit is abbreviated to CPU and a random access memory is abbreviated to RAM. When recognizing that the touch operation or the proximity operation is performed on or to the touch screen 102, the CPU 110 receives this operation as an input operation and performs processing according to an input operation.” EX1008, 4:61-5:4.

81. Different touch operations that Miyazawa discloses the controller executes based on detection of the user's finger touch include "dragging" (EX1008, 7:33-38), "flicking" and "tapping" (EX1008, 7:54-62); and pinching (EX1008, 15:44-56).

D. Rekimoto (EX1010)

82. U.S. Patent No. 8,477,115 ("Rekimoto") was filed on June 7, 2006 and published July 2, 2013. I am informed that Rekimoto is prior art to the '086 patent under 35 U.S.C. §102(e).

83. Rekimoto discloses inputting input information by a pad of the finger ("finger pad") and inputting input information by an end of the finger ("fingertip"):

FIGS. 2A and 2B are a schematic sectional view and a plan view both showing the control panel (the surface of the contact sensor section 2) of an input section of the input device 1 which a user presses by erecting a finger and thus with a *fingertip*.... FIGS. 3A and 3B are a schematic sectional view and a plan view both showing the control panel (the surface of the contact sensor section 2) of the input device 1 which the user presses by laying down the finger and thus with the *finger pad*....

EX1010, 5:13-24.

FIG.2A

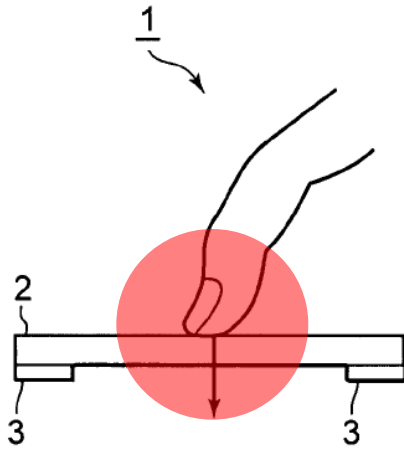
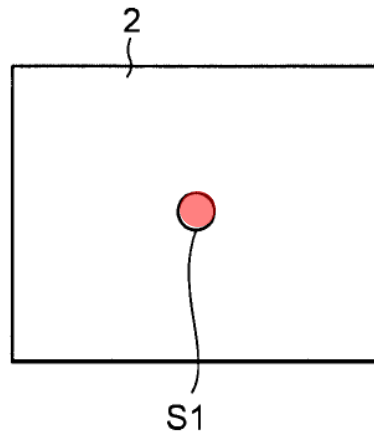


FIG.2B



EX1010, FIGS. 2A, 2B.

FIG.3A

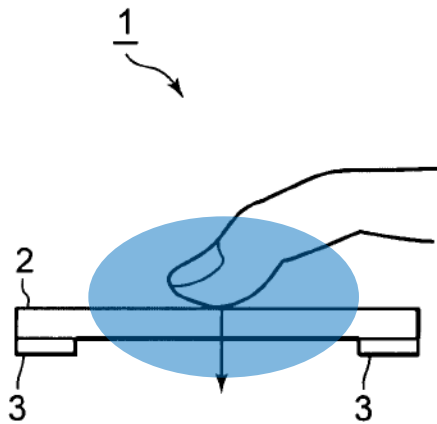
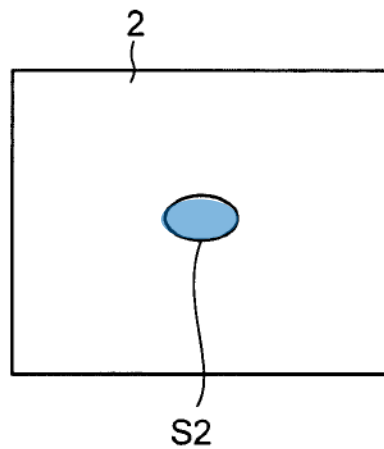


FIG.3B

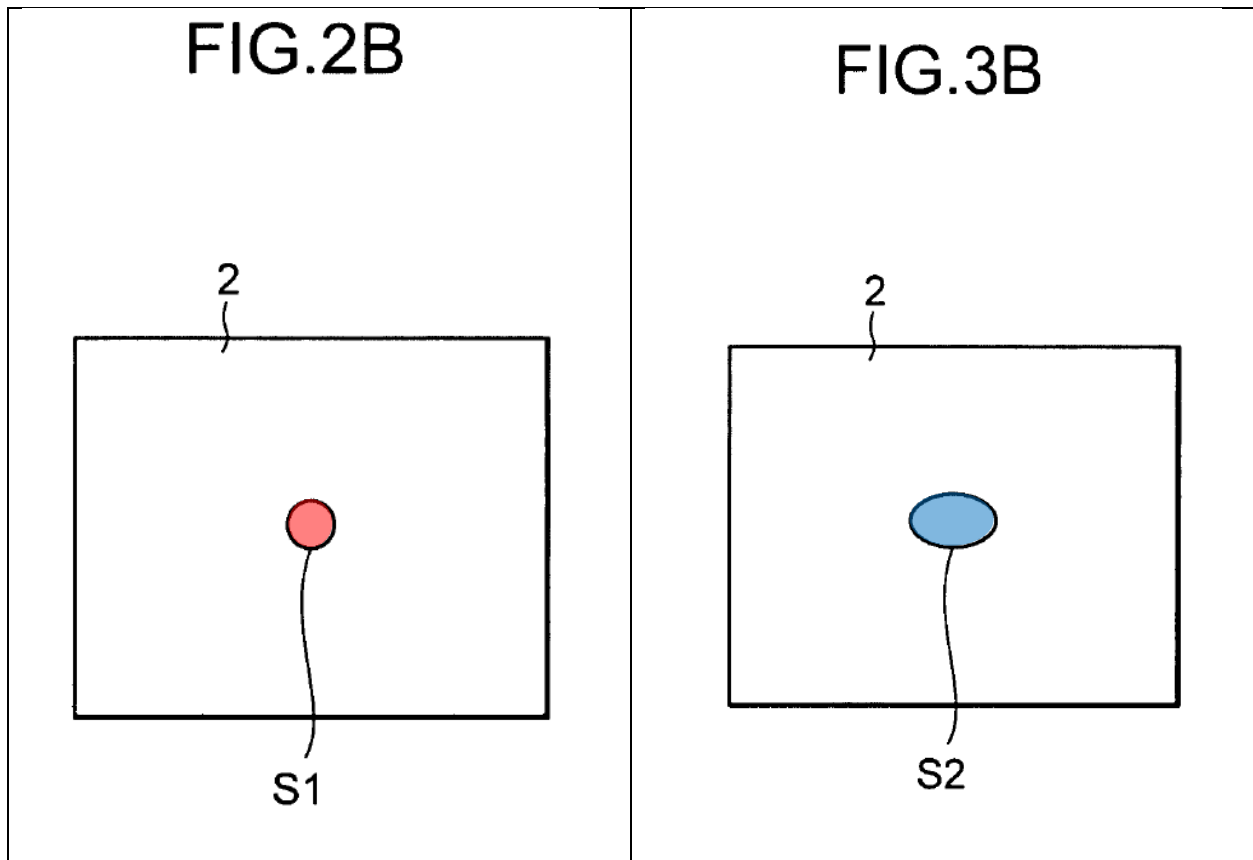


EX1010, FIGS. 3A, 3B.

84. Rekimoto explicitly discloses distinguishing fingertip touches and finger pad touches:

During the input operation, the *contact area of the contact sensor section 2 occupied by the fingertip equals a small area S1...* The contact area of the contact sensor section 2 touched by the *finger pad equals a large area S2...* That is, compared with the area S1, which is an area of the contact sensor section 2 surface touched by the fingertip, the area S2 touched by the finger pad is larger (wider). *These areas S1, S2 can be clearly distinguished by using a threshold St of a specified area as a boundary.*

EX1010, 5:18-31.



85. Rekimoto discloses that fingertip and finger pad touches can be used for different processing (zoom operations in the illustrated example): “Therefore, by pressing the input device 1 by erecting a finger and thus with a fingertip, the user can perform first processing for zooming in on an image in response to the pressing force. Similarly, by pressing the input device 1 by laying the finger down and thus with the finger pad, the user can perform second processing for zooming out on the image in response to the pressing force.” EX1010, 5:31-37.

**X. GROUND 1: THE COMBINATION OF ROGERS AND ROSENBERG
RENDERS CHALLENGED CLAIMS 1, 2 AND 4-7 OBVIOUS**

A. Motivation to Combine Rogers with Rosenberg

86. In my opinion, a POSITA would have found it obvious to combine the teachings of Rogers and Rosenberg. Both references are directed to allowing users to input information via touchsurface² technology, in which they are both analogous art to the '086 patent. EX1006, Abstract, FIGS. 1, 2A; EX1007, Abstract, FIG. 1. For example, Rosenberg discloses that the use of both finger end and finger pad touch is “natural and intuitive” for users, and teaches distinguishing the use of a finger pad/finger end by relying “upon the orientation in which the user’s finger engages the touch screen.” EX1007, ¶28. Enabling such input “in a particularly natural and intuitive manner” is consistent with one of the '086 patent’s stated goals of “offer[ing] improved convenience to users.” EX1007, ¶28, EX1001, 1:34-36.

87. Thus, it is my opinion that a POSITA would have found Rogers and Rosenberg to be compatible because of the technical similarity of their teachings, and a POSITA would have further recognized that Rosenberg’s finger orientation disclosures, applied to Rogers’ graphical passcode disclosures, would facilitate a

² The terms “touchscreen/touchsurface” may also be referred to as “touch screen/touch surface” or “touchScreen/touchSurface” as Rogers makes clear that “a ‘touchscreen’ is a touch input device Touchscreens and touchpads are generically referred to herein as ‘touchsurfaces.’” EX1006, 3:4-10.

“natural and intuitive” means of implementing the teachings of Rogers. A POSITA, in my opinion, would therefore have been motivated to look to Rosenberg to improve Rogers, and vice-versa.

88. Rogers teaches distinguishing between a “large fingertip and a small stylus tip” based on “area difference[s]” between the two input types as a factor in graphical passcode authentication. EX1006, 7:59-62. A POSITA would have recognized that this implementation goal would have been better accomplished through Rosenberg’s teachings of distinguishing finger pad touches from fingertip touches. Rosenberg expressly states that “a stylus is often not always preferred because it requires that the user employ another piece of hardware that needs to be stored, taken out of a holder for usage, put away after usage, and is often accidentally lost,” and that “a stylus is often not convenient for touch screen interfaces that enable multipoint targeting and multi-finger gesturing because a user can not easily hold a stylus at the same time he or she is performing a multi-finger gesture.” EX1007, ¶30. A POSITA therefore would have considered the disclosures in Rosenberg and been motivated to modify Rogers’ “large fingertip and a small stylus tip” example so that it instead used the “natural and intuitive” finger pad versus finger end distinction discussed in Rosenberg. A POSITA, in my opinion, would have found this modification to be a simple substitution of elements well known in the art requiring only routine skill, and would have had a

reasonable expectation of success in achieving the benefits disclosed in Rosenberg by making the modification.

89. Moreover, it is my opinion that adding finger end and finger pad touch detection to Rogers would involve no more than applying a known technique (i.e., finger end and finger pad touch detection/distinction as taught by Rosenberg) to a known device ready for improvement (Rogers' apparatus having "large fingertip and a small stylus tip" capabilities) to yield predictable results (a simple-to-use touch screen interface with multipoint targeting and multi-finger gesturing). It is my understanding that these are all proper rationale for an obviousness determination.

90. In my opinion, it would also have been obvious to combine Rogers with Rosenberg because both references disclose touch screen interfaces that detect a contact area of a finger. Rogers discloses that the "measurable parameters" of a "template graphical passcode" can include "contact area." EX1006, 4:15-19. Rosenberg teaches distinguishing between finger pad and finger end touches by "size, shape, and/or orientation of the detected finger." EX1007, ¶50. Rosenberg further explains how this may be accomplished, namely that "finger-tip interaction" and "finger-pad interaction" are "generally easily distinguishable for a given finger of a given user because the finger contact area caused by a finger-tip interaction is substantially smaller in total area, often narrower in shape (i.e., a

more eccentric ellipse), and usually has the major axis orientated such that it extends in a direction across the width of the user's finger." EX1007, ¶49. A POSITA in my opinion would have considered Rosenberg's disclosures and been motivated to modify the "graphical passcode" features of Rogers so that the disclosed device is capable of detecting information input by a pad or end of a finger, because it would provide a "generally easily distinguishable" basis upon which to program the device disclosed in Rogers to detect a "measurable parameter" based on "contact area."

91. It is also my opinion that a POSITA would have further recognized that these features of Rogers and Rosenberg could be successfully combined because both references teach a "calibration" mode in which the user trains the device to recognize a specific range of input parameters that allows for some variation in input while remaining within acceptable tolerances. EX1006, 4:48-62 (describing "training sessions"), EX1007, ¶49 (describing a "calibration routine"). Because a user can readily distinguish between a finger end and a finger pad when performing input, and because Rosenberg teaches the ability to "easily distinguish[]" between a finger end and a finger pad, it would have been obvious to modify Rogers (to the extent not already taught) to receive input information indicating the use of a pad or end of a finger. Because Rogers also teaches that the contact area on the touchscreen may be one of the parameters for the graphical

passcode, Rogers expressly suggests to a skilled artisan the ease of making the modification to detect the end/pad of a finger, and that the area of contact is a desirable parameter for inputting an authentication passcode. A POSITA in my opinion would have had a reasonable expectation of success in modifying Rogers in this manner for at least the same reasons. It is my understanding that these are also all proper rationale for an obviousness determination.

B. Claim 1

1. [1pre] “An information processing apparatus comprising:”

92. To the extent the preamble is considered limiting, it is my opinion that Rogers discloses it. Rogers discloses that its embodiments may be implemented “on various computer or electronic devices, including cellular phones, laptop computers, personal digital assistants (PDAs), smart phones, desktop computers, gaming consoles and the like.” EX1006, 1:62-66; 3:14-28; 5:6-48; FIG. 1:

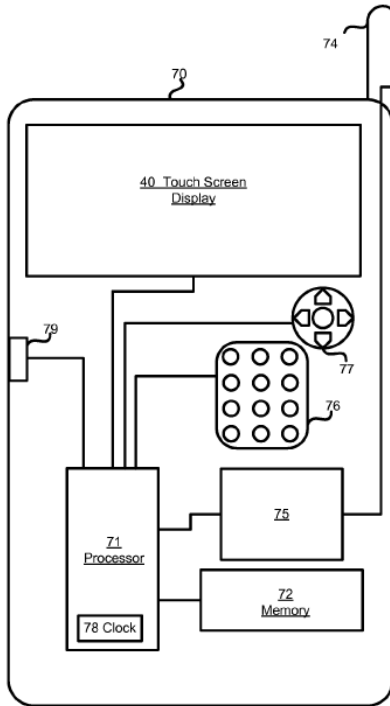


Fig. 1

EX1006, FIG. 1.

2. [1a] “a touch panel configured to detect a contact of a finger of a user;”

93. It is my opinion that Rogers discloses limitation [1a]. In one example, Rogers discloses a “touch screen display 40” as one of the “typical components” of exemplary “electronic device 70.” EX1006, 5:6-16; FIG. 1.

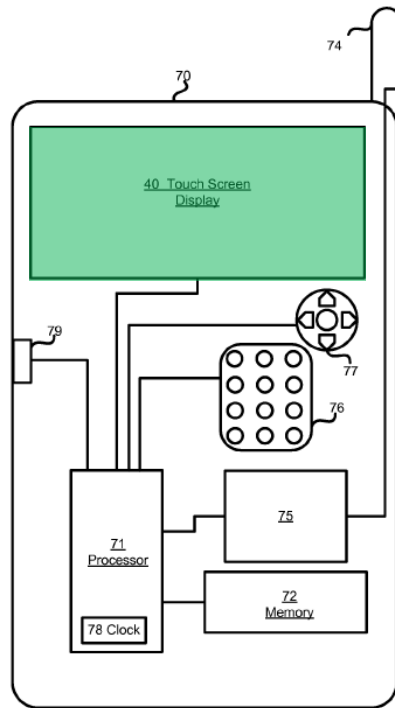


Fig. 1

EX1006, FIG. 1.

94. Rogers discloses that the “touch screen display 40 can be any type of touch screen,” and explains that a user may “draw[] a finger tip across the touchsurface” to “input[] a graphical passcode.” EX1006, 5:11-27, 8:46-49. For example, Rogers discloses, “[a] method and system for electronic access security [that] uses touches and movements on a touch sensitive surface to determine graphical passcode that are used in a manner similar to passwords.” EX1006, Abstract. “Various embodiments provide methods and systems for reliably and rapidly identifying graphical passcodes and/or identifiers entered on a touchscreen or touchpad of an electronic device.” EX1006, 1:35-38; *see also* 1:45-50; 3:32-39; 7:56-62; 8:44-49; 10:4-10.

3. **[1b] “a detector configured to detect first information necessary for an identification of the user when the contact is detected between the touch panel and the finger of the user;”**

95. It is my opinion that Rogers discloses limitation [1b]. For clarity, I have broken down this limitation into “first information necessary for an identification of the user” and “a detector configured to detect ... when the contact is detected between the touch panel and the finger of the user.” I explain how Rogers satisfies each of these requirements in the paragraphs below.

first information necessary for an identification of the user

96. For this part of the limitation, Rogers discloses the “graphical passcode” entered by the user’s finger touch and captured by the device during an “authenticating” process illustrated in FIG. 5. This “graphical passcode” satisfies the claimed “first information.” Furthermore, Rogers discloses that “when a user requests access to the secured electronic device, the user is prompted to enter the graphical passcode.” EX1006, 1:53-55. “The user then inputs the graphical passcode *by touching the touchscreen or touchpad* in the same memorable manner” that matches the same “measurable parameters” as the user’s previously registered passcode that had been stored in memory. EX1006, 1:46-55. As Rogers explains, “The measurable parameter of the input graphical password is measured, and compared with the envelope [(e.g., pressure, speed)] of the parameter stored in memory.” EX1006, 1:57-60. This matching process is used to identify the user:

“Access is provided if the measured parameter falls within the envelope.” EX1006, 1:45-61.

a detector configured to detect ... when the contact is detected between the touch panel and the finger of the user

97. For this second part of the limitation, Rogers discloses that the “electronic device 70” can include “sensors for detecting and measuring the pressure or force applied to the touchscreen 40.” EX1006, 5:28-30. Specifically, Rogers discloses detecting finger contact through taking “a measurement of a size (i.e., area) of the object *or fingertip* applied to the touchsurface.” EX1006, 7:56-59. Accordingly, Rogers explicitly discloses that the sensors are detectors configured to detect first information necessary for an identification of the user when the contact is detected between the touch panel and the finger of the user.

98. Moreover, Rogers at 13:28-59 discloses support for a variety of additional sensing technologies that “touchscreen 40” may use for detecting the input of a user’s graphical password, including “resistive, Surface Acoustic Wave, Capacitive, Infrared, Strain Gauge, Optical Imaging, Dispersive Signal technology, acoustic pulse recognition, and frustrated total internal reflection.” EX1006, 13:30-35. Rogers also discloses that:

Regardless of which touchscreen technology is implemented, when a user touches a particular point on the touchscreen 40 panel, an

electrical signal may be sensed and converted into an interrupt signal by a hardware driver layer 50. The hardware driver 50 is a firmware program that converts signals from the touchscreen 40 into data signals which can be stored and interpreted by software applications.

EX1006, 13:60-68.

99. With respect to the claimed “first information necessary for the identification of the user” (e.g., graphical passcode), Rogers further discloses that the processor 71 measures the parameters of the inputted graphical passcode for comparison with the graphical passcode template that was previously stored in memory (e.g., during training by the user). EX1006, 9:1-28. Regarding the user’s finger, Rogers discloses taking “a measurement of a size (i.e., area) of the object or fingertip applied to the touchsurface.” EX1006, 7:56-59. Thus, Rogers discloses that the sensors of the touchscreen 40, the sensors in conjunction with the hardware driver layer 50, and/or the sensors in conjunction with the hardware driver layer plus the processor 71 are configured to detect the graphical passcode when the contact is detected between the touch panel and the finger of the user.

4. **[1c] “a first controller configured to control the information processing apparatus to operate into two operating modes:**

at least an identification mode and a registering mode, as the operating mode thereof;"

100. Rogers, in my opinion, discloses limitation [1c]. Rogers discloses a “processor 71,” which is a controller that controls “electronic device 70” to operate in two operating modes. The first mode is a registration mode for “initializing an electronic device with a template graphical password.” The second mode is an identification mode for “using graphical passcodes to gain access to an electronic device.” EX1006, 8:42-49; FIG. 4 (initializing steps); 9:29-36; FIG. 5 (authenticating process with gain access steps); *see also* Abstract; 1:45-61; 3:57-4:14; 5:16-27.

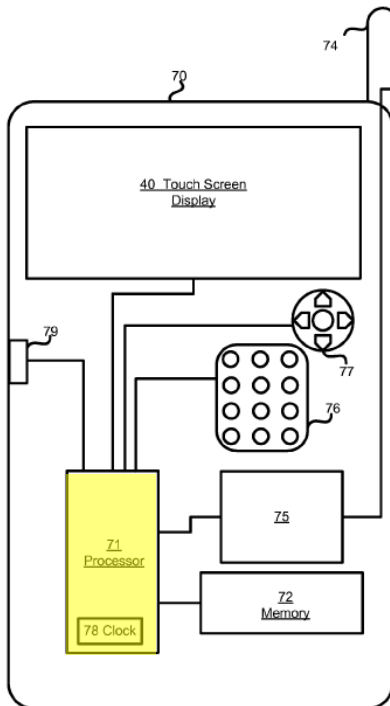


Fig. 1

EX1006, FIG. 1.

101. The process disclosed by Rogers' FIG. 5 (described as "authenticating a graphical passcode") is the claimed "identification mode." This figure shows the process flow controlled by processor 71 "for using graphical passcodes to gain access to an electronic device." EX1006, 9:29-31; 2:32-33. Moreover, Rogers' explanation of this figure further explains the "identification mode." Rogers explains that "[t]he electronic device 7 via the processor 71 and display 40 prompts the user to input a graphical passcode that is being used as an authentication credential, step 203." EX1006, 33-36; FIG. 5:

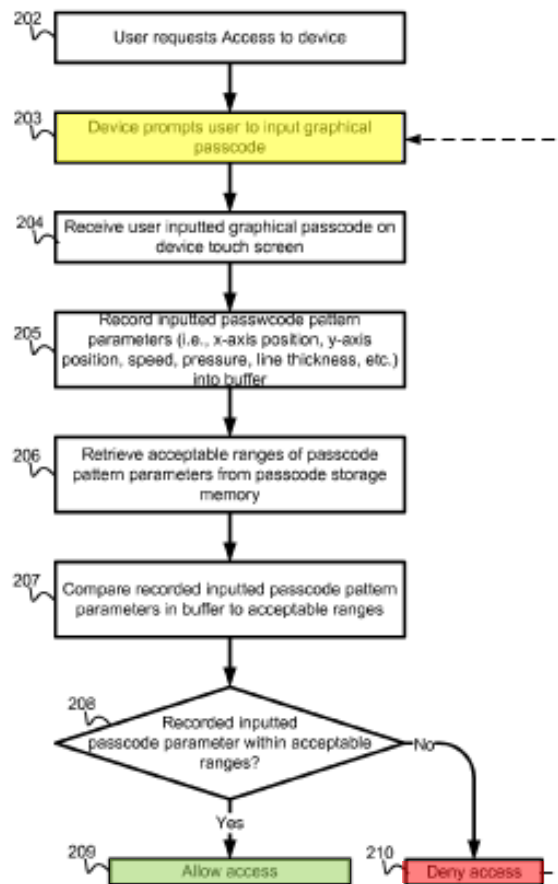


Fig. 5

EX1006, FIG. 5.

102. As part of an authentication process, the user enters a graphical passcode on the touch surface, and “processor 71 measures various characteristic parameters (*e.g.*, pressure, force, speed, X or Y coordinate data) of the inputted graphical passcode and stores the measured parameter values in a memory buffer, step 205.” EX1006, 9:38-42. At step 207, the entered graphical passcode and parameters are compared to the “graphical passcode template” that was previously stored. EX1006, 9:54-57. At step 208, the processor 71 determines whether the inputted graphical passcode matches, or is within an acceptable range of, the graphical passcode template. EX1006, 9:57-60. If there is a match, the user is allowed access to the device; if there is no match, the user is denied access to the device. EX1006, 9:50-10:1.

103. Moreover, the claimed “registration mode” is satisfied by the process disclosed by Rogers’ FIG. 4. The process in this figure shows another mode of operation wherein the processor 71 controls the electronic device 70 to initialize, *i.e.*, “creating and storing,” a “template graphical passcode.” For example, “[t]he electronic device 70 *via the processor 71* and display 40 may prompt a user to input a desired graphical passcode, step 101.” EX1006, 8:44-46. At step 102, “the user inputs a graphical passcode to be used as a passcode template, . . . such as by drawing a finger tip across the touchsurface in the appropriate manner.” EX1006,

8:42-49. The process is repeated several times in a training session at steps 103 and 104, so that the device can measure and learn the typical variations when the user enters the graphical passcode. EX1006, 8:49-67. Once the graphical passcode and parameters are determined, the graphical passcode is stored in memory. EX1006, 9:22-25. “The passcode template and its acceptable envelope values are used by the processor 71 to determine the authenticity of a subsequently inputted graphical passcode” (in the identification mode). EX1006, 9:25-28.

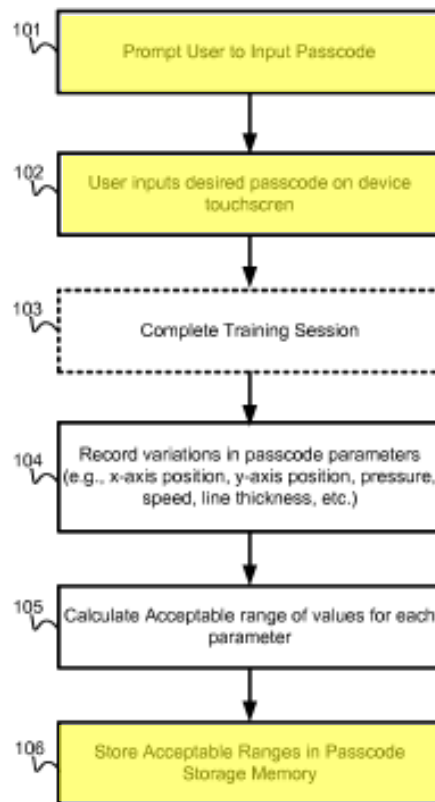


Fig. 4

EX1006, FIG. 4.

5. [1d] “memory that is configured to store second information relating to the identification of the user, which is stored in advance; and”

104. It is my opinion that Rogers discloses limitation [1d]. For clarity, I have broken this limitation up into “second information relating to the identification of the user” and “memory configured to store the second information in advance.” I explain how Rogers satisfies each of these requirements in the paragraphs below.

second information relating to the identification of the user

105. For this part of the claim limitation, Rogers discloses the “graphical passcode” created and stored based on the user’s finger touch captured by the device during the “creating and storing a desired graphical passcode” process illustrated in FIG. 4. This “graphical passcode” is the claimed “second information.” In more detail, Rogers discloses that “[a] user’s selected graphical password is stored in memory for comparison to subsequent entries of graphical passcode in order to authenticate the users.” EX1006, Abstract. Rogers also discloses authenticating of a user that is the claimed “identification of the user” as required by the ’086 patent: “The graphical passcode is used as a password, personal identifier, or key to provide secure access to an electronic device, network, website or the like.” EX1006, 3:32-39, 13:14-20 (see especially “The

present graphical passcodes . . . can be used to lock or unlock an electronic device .
. . . or identify an individual to an electronic device, network or website.”).

memory configured to store the second information in advance

106. For this part of the limitation, Rogers discloses an electronic device 70 that has “a computer readable memory 72.” EX1006, 5:6-11; FIG. 1:

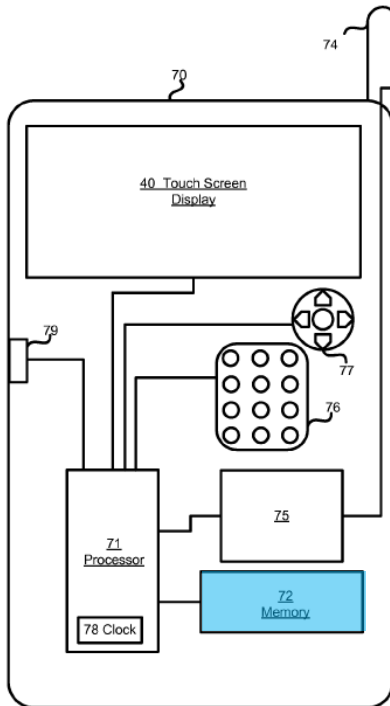


Fig. 1

EX1006, FIG. 1.

107. Rogers discloses storing the graphical passcode in memory 72. As explained above, the graphical passcode is “second information relating to the identification of the user.” EX1006, 5:19-21. Moreover, the storage of the graphical password is “in advance” because the authentication process occurs “subsequent” to the storage process:

Subsequently, each time a user wishes to access the electronic device 70, the users provides the graphical passcode to the electronic device 70 via the touch screen 40. The processor 71 compares the subsequently inputted graphical passcode to the template graphical pass code and associated plots or datasets (*i.e.*, one or more envelopes) stored in the memory 72 as described more fully below.

EX1006, 5:21-27; *see also* 8:41-67 (“The electronic device 70 processor 71 measures at least one characteristic parameter of the inputted template graphical passcode and stores the measured at least one characteristic parameter in the internal memory 72 as at least part of the passcode template, step 104.”); 9:22-28 (“Once the acceptable envelope values have been calculated, the acceptable envelope values *are stored in the memory 72* as part of the passcode template, step 106. The passcode template and its acceptable envelope values are used by the processor 71 to determine the authenticity of a *subsequently* inputted graphical passcode.”); 9:36-51.

6. [1e] “a second controller configured to execute a specified process when said first information and said second information are coincident within said identification mode, wherein:”

108. It is my opinion that Rogers discloses or renders obvious limitation [1e]. Rogers discloses that processor 71 can be implemented in hardware as “processing elements” (plural):

The hardware used to implement the forgoing embodiments may be *processing elements* and memory elements configured to execute a set of instructions, wherein the set of instructions are for performing method steps corresponding to the above methods. Alternatively, some steps or methods may be performed by *circuitry that is specific to a given function*.

EX1006,13:21-27; *see also id.* 14:28-40.

109. Rogers also discloses that processor 71 can be either hardware or software, or even some combination of both:

Those of skill in the art would appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein *may be implemented as electronic hardware, computer software, or combinations of both....*

EX1006, 14:41-55; *see also* 14:56-15:4 (disclosing that embodiments of a method or algorithm—singular—may be embodied in “hardware, software modules, or a combination of the two.”).

110. In my opinion, a POSITA would have understood and continue to understand that Rogers discloses that functions of processor 71 could be split into multiple components including multiple hardware processing elements, multiple software modules, or a combination of software modules combined with hardware processors and circuits.

111. It is also my opinion that a POSITA would have understood that Rogers discloses that the separate processes performed by processor 71 are

disclosed as being performed by *separate* processing elements, each of which could be run on a separate module as discussed above. Thus, a POSITA would have understood that these multiple processing elements running on separate modules are the claimed multiple controllers.

112. Regarding the claimed “execut[ing] a specified process when said first information and said second information are coincident with said identification mode,” Rogers discloses that a processing element of processor 71 (“second controller”), unlocks the electronic device 70 (“specified process”) when the entered graphical passcode (“first information”) matches the stored graphical password template (“second information”). EX1006, 5:16-27; *see also* 8:42-9:28, and FIG. 4 (illustrating registration of graphical password template); 9:29-10:3, and FIG. 5 (illustrating authentication of user to unlock device by matching entered graphical password to previously stored graphical password template).

113. In my opinion, a POSITA would have understood that Rogers discloses that the processing element, including the software and/or hardware components, of processor 71 that unlocks the device 70 can be a different processing element, including different software and/or hardware components, than the processing element that performs the functions of limitation 1[c] discussed above.

114. To the extent that Patent Owner argues that Rogers does not explicitly disclose a second controller, it is my opinion that a POSITA would have found it obvious to include it. Specifically, a POSITA would have found it obvious to modify Rogers to have a second controller configured to execute the specified process of this limitation. Because Rogers suggests, as I have detailed in Rogers teachings above, that multiple hardware/software components, or a combination of the two, can be used to implement a controller and the associated functional steps, including the passcode authentication process disclosed in FIG. 5, a POSITA would have found it obvious to try this modification. Rogers discloses that using two or more hardware and/or software components to perform the functions of a single component (i.e., using two controllers instead of one controller) is a simple substitution: specifically, taking a single controller and replacing it with multiple controllers that collectively perform the same functions. Rogers further discloses that a POSITA would have had a reasonable expectation of success in making the substitution by disclosing that the “illustrative components, blocks, modules, circuits, and steps” described in the specification were described “to clearly illustrate th[e] interchangeability of hardware and software.” EX1006, 14:45-49. Moreover, it is my opinion that a POSITA would have been motivated to make this change to improve device security by separating the processor functions of the device that were responsible for authenticating a user via stored data from other

generalized device functions such as selecting applications or programs/processes that do not implicate these security features. It is my understanding that these are all proper rationale for an obviousness determination.

7. **[1f] “in said registering mode, there are provided a first registering mode for inputting input information by a pad of the finger, and a second registering mode for inputting input information by an end of the finger, and said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode.”**

115. It is my opinion that the Rogers or the Rogers-Rosenberg combination renders limitation 1[f] obvious. For clarity, I have broken this limitation up into “first registering mode... and second registering mode...” and “said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode.” In the following paragraphs, I explain how Rogers and Rogers in view of Rosenberg discloses these two requirements.

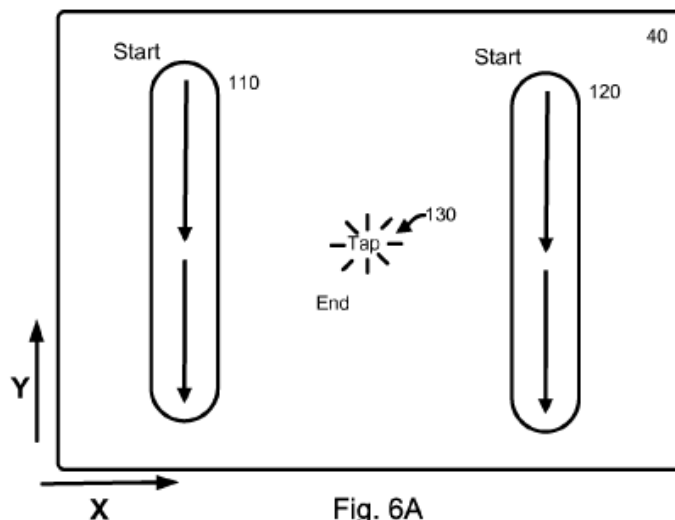
first registering mode (finger pad input) and second registering mode (finger end/tip input)

116. First, Rogers discloses two registering modes that distinguish between inputting two different types of user input. Rogers discloses prompting the user to enter the graphical passcode and measuring various parameters with which the passcode is entered. This causes a graphical passcode template to be registered.

EX1006, 3:32-39, 4:15-19 (“The graphical passcode is essentially a series of touches, swipes and/or taps on a touchsurface” that are inputted with “one or more measurable parameters (e.g., timing, speed, pressure, force, line thickness, contact area, or location)...”).

117. Alternatively or additionally, Rogers discloses that the “inputted graphical passcode may employ a measurement of a size (i.e., area) of the object or fingertip applied to the touchsurface,” allowing the touchsurface, for example, to “discriminate between a large fingertip and a small stylus tip.” EX1006, 7:56-62. Rogers discloses that “[a]uthentication may require a measured contact area greater than or less than a certain size, or within a certain size range.” EX1006, 7:56-67.

118. FIG. 6A shows an example of a graphical passcode that “consists of two simultaneous swipes 110, 120 (e.g., made with two fingers), followed by a tap 130 in the middle of the touch surface.” EX1006, 10:8-10.



119. FIG. 6B of Rogers illustrates using pressure to measure the width and position of the two finger swipes 110 and 120:

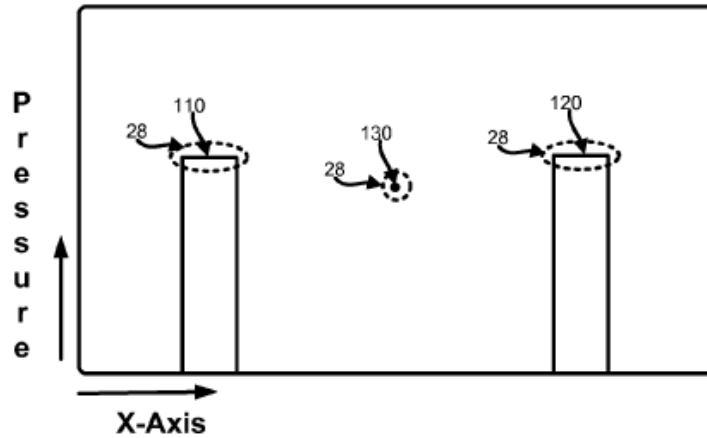


Fig. 6B

120. Rogers further discloses that line thickness is the contact area between the finger and the touch screen, EX1006, 3:52, and that a capacitive sensor can be used to measure the width of finger touch. EX1006, 1:66-2:3, 5:11-14, 13:27-35, 13:51-59.

121. Additionally, Rogers' discussion of FIG. 7 makes it clear that different measurements taken of the same type of input parameter can be stored for touches at different positions on the touch screen. EX1006, 10:44-48, FIGS. 7A (illustrating graphical passcode entered by 5 taps), 7B (illustrating varying pressures with X-position), 7C (illustrating varying pressures with Y-position), 7D, 7E (illustrating pressure versus time for all 5 taps). As explained above, Rogers discloses that the size or area of the fingertip measured by the touch screen can be used instead of or in addition to pressure, it is my opinion that a POSITA would

have understood that Rogers discloses that the registration of a graphical passcode can discriminate between smaller and larger contact areas of the user's finger as well as different positions on the touch screen. In other words, Rogers discloses separate registering modes for entering different pieces of user information based on the size measured from the contact area of the user's touch. Thus, Rogers' disclosure of registering a graphical passcode that distinguishes between small and large contact areas corresponds to the first and second registration modes.

122. In another example, Rogers further discloses two registration modes in the form of the "training session" for developing the thresholds, ranges or envelopes, and the measured parameters such as line thickness. This is a registration mode as it involves repeated entry of the passcode to create thresholds for distinguishing between the different measured parameters, such as line thickness or contact area, for the touch inputs that make up the desired passcodes. EX1006, 8:42-67. The measured passcode parameters can include things like "line thickness" or area, and be stored based at least in part on the position of the input on the touch screen. EX1006, 8:59-67. So, for example, a training session that creates a threshold for a narrow line thickness or small area at one position and a threshold for a wide line thickness or large area at another position, correspond to the first and second registration modes required by the claim.

123. Rogers discloses or renders obvious that the different user input information input entered in the two claimed registration modes include a pad of the finger and an end of the finger. Rogers discloses that finger touches are some of the types of user input information, among others, that the disclosed graphical template can distinguish between. As discussed above, “contact area” or “line width” is a detected parameter that Rogers discloses can be distinguished during input measurement of finger touches. EX1006, 7:56-67. It is my opinion that a POSITA would have understood that Rogers’ disclosures related to contact area and line width would distinguish between different fingers or portions of a finger. EX1006, FIGS. 6A-6E.

124. A POSITA would have also understood that Rogers’ disclosures are virtually identical to the “modes” of the ’086 patent’s preferred embodiment of this claim limitation. The ’086 patent describes identifying finger pad input from finger tip input based on differences in measurements between a small contact range and a wider contact range. EX1001, 3:3-13. Thus, Rogers’ disclosure of discriminating between a small contact area or line width and a large contact area or line width expressly discloses “finger tip input” and “finger pad input” as those terms are used for the preferred embodiment of the ’086 patent.

said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode

125. The claim limitation also requires that the second information related to identification of the user must be produced by inputting information in “at least” one of the first or second modes (presumably the registering modes required by the claim). In other words, the second information (e.g., the passcode as described above) must include at least a measurement of narrow contact range (i.e., fingertip input) or a wide contact range (i.e., finger pad input), but the claim language does not require both. Rogers expressly discloses the discrimination between narrower and wider contact areas and that at least one of the narrow or wider contact ranges can be used when registering a graphical passcode, thus disclosing this requirement of the claim. The narrow or wider contact range information, is stored, or created, or “produced,” when the user inputs information in the first or second registration mode as discussed above. EX1006, 7:56-67 (See especially, “Authentication may require a measured contact area greater than or less than a certain size, or within a certain size range. The size requirement can be determined during a training session, or can be predetermined or can be selected by the user.”). Additionally, Rogers discloses an example that includes recording the contact area width as part of the graphical passcode registration process. EX1006, 10:4-15, FIGS. 6A, 6B.

Rogers in view of Rosenberg

126. To the extent Patent Owner argues that Rogers does not fully disclose limitation [1f] because Rogers does not explicitly recite the use of “finger pad” and “finger tip” inputs, it is my opinion that Rogers in view of Rosenberg renders this limitation obvious.

127. Rosenberg explicitly discloses inputting input information by a pad of the finger (“pad-pointing”) and also inputting input information by an end of the finger (“tip-pointing”). As Rosenberg states, “embodiments of the present invention are operative to distinguish between finger-tip interactions (referred to herein as “tip-pointing”) where the user engages the touch screen with the tip of his or her finger and finger-pad interactions (referred to herein as “pad-pointing”) where the user engages the touch screen with the pad of his or her finger.”

EX1007, ¶30. According to Rosenberg, “a variety of methods for distinguishing between finger-tip interactions and finger-pad interactions, including an assessment of the finger contact area size, shape, and/or orientation” are used to “enable mode selection in a particularly natural and intuitive manner, based upon the orientation in which the user’s finger engages the touch screen.” EX1007, ¶¶27, 28, 45.

128. Moreover, Rosenberg explicitly discloses identifying pad-pointing as opposed to tip-pointing “[b]ased upon the size and/or shape” of the contact area (shown as an ellipse A’ in FIG. 6):

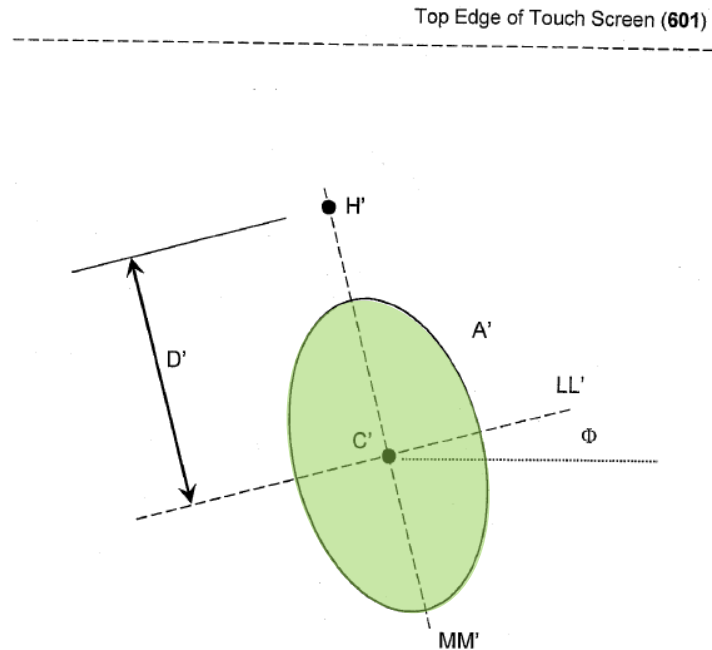


Fig. 6

EX1007, FIG. 6. Rosenberg provides an example in which pad-pointing is shown in FIG. 8A and tip-pointing is shown in FIG. 8B. EX1007, ¶50.

Fig 8a

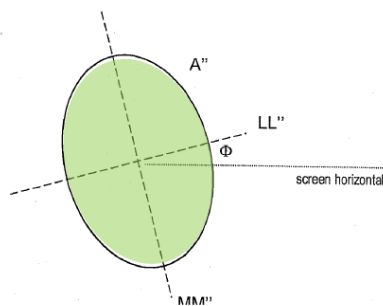
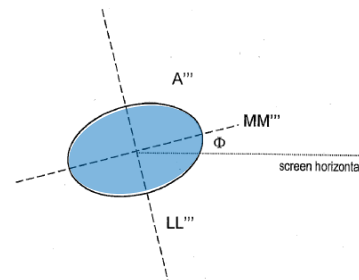


Fig 8b



129. By way of additional detail, Rosenberg explains that the tip-pointing interaction (FIG. 8B) “is substantially smaller in size (both area and circumference), more eccentric in shape (i.e., less rounded), and is oriented such that the major axis MM’’ is oriented closer to the reference screen horizontal.” EX1007, ¶50. Furthermore, the pad-pointing contact (FIG. 8A) “is substantially larger in size (both area and circumference), is less eccentric in shape (i.e., more rounded), and is oriented such that the minor axis LL’’ is oriented closer to the reference screen horizontal.” EX1007, ¶50. “Thus, each of the size, shape, and/or orientation of the detected finger contact area may be used alone or in combination by the routines of the present invention to distinguish between a tip-pointing interaction and a pad-pointing interaction.” EX1007, ¶50.

C. Claim 2 “The information processing apparatus according to claim 1, wherein said first information includes a position and an area of the finger contacting with said touch panel.”

130. The Rogers-Rosenberg combination renders claim 1 obvious as discussed above. §X.B. As also explained above, Rogers also discloses “first information,” §X.B.3. Additionally, it is my opinion that Rogers discloses “said first information includes a position and an area of the finger contacting with said touch panel” as required by Claim 2.

131. Specifically, Rogers discloses that “when the template graphical passcode is inputted, one or more measurable parameters (e.g. timing, speed,

pressure, force, line thickness, *contact area*, or *location*) of the inputted template graphical passcode is measured by the touchsurface. The measured parameters may be plotted as a function of time and/or position on the touchsurface.” EX1006, 4:15-21. “When a graphical passcode is subsequently inputted, the same parameters are measured and plotted as a function of time and/or position and compared to the plots of the template graphical passcode.” EX1006, 4:27-30; *see also* 3:48-56 (“‘envelope’ refers to a range of a parameter within a graphical passcode that accounts for the inherent variability in such passcodes. The parameter can be, for example, pressure, force, speed, *X-axis position*, *Y-axis position*, or *line thickness (i.e. contact area)*.”), 7:56-67.

D. Claim 4 “The information processing apparatus according to claim 1, wherein said specified process includes releasing of a lock of resting an operation of said information processing apparatus.”

132. The Rogers-Rosenberg combination renders claim 1 obvious as discussed above. §X.B. As also discussed above, Rogers discloses the “specified process.” §X.B.6. It is also my opinion that the Rogers discloses or renders obvious that “said specified process includes releasing of a lock of resting an operation of said information processing apparatus” as required by Claim 4.

133. Specifically, Rogers discloses that “graphical passcodes can be used in the same manner that conventional passwords, security codes or personal identifiers are currently used” and explicitly discloses that “the passcodes can be

used to lock or unlock an electronic device.” EX1006, 13:14-17. Rogers also discloses or renders obvious that the processing element of processor 71 (“second controller”) unlocks the electronic device 70 (“specified process”) when the entered graphical passcode (“first information”) matches the stored graphical password template (“second information”) to provide the user access to the device. EX1006, 5:16-27; 9:29-10:3, FIG. 5. A POSITA in my opinion would have understood that a locked device is in a resting operation and that unlocking the device releases the lock of the resting operation.

E. Claim 5 “The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display a first image and first descriptive text associated with the first registering mode and a second image and second descriptive text associated with the second registering mode.”

134. The Rogers-Rosenberg combination renders claim 1 obvious as discussed above. §X.B. As also discussed above, Rogers in view of Rosenberg renders obvious the inputting of second information relating to the identification of the user in the first or second registering mode, §X.B.7. It is also my opinion that the Rogers-Rosenberg combination renders obvious the additional requirements of Claim 5. Moreover, Rogers discloses that its touch panel 40 includes a display. EX1006, 3:4-5 (“As used herein, a ‘touchscreen’ is a touch input device with an associated image display.”), 5:6-16:

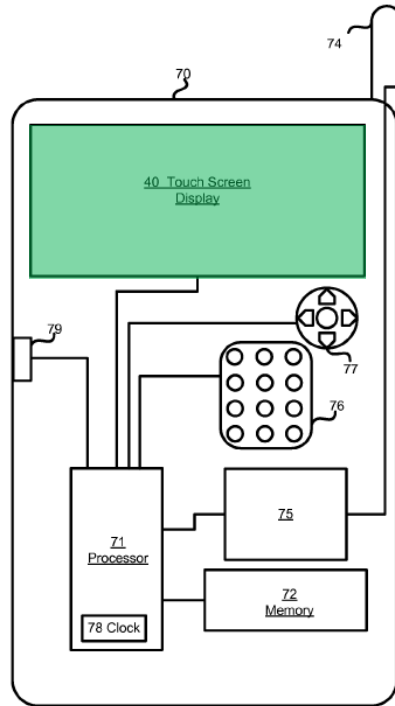
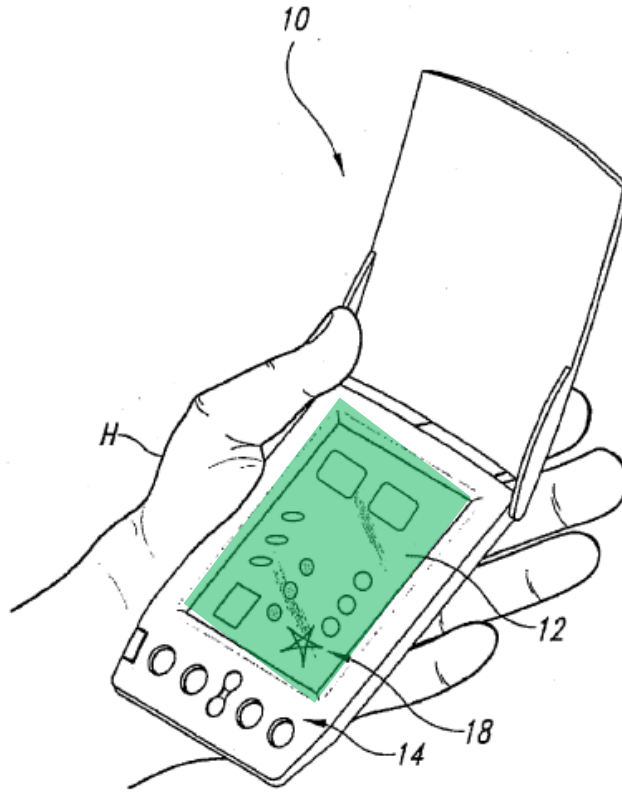


Fig. 1

EX1006, FIG. 1.

135. Rosenberg also discloses that its handheld computer includes a “display screen 12 [that] is a touch screen that is used as the primarily controls the operation of the computer 10.” EX1007, ¶30; FIG 1:



EX1007, FIG. 1.

136. Rosenberg's display screen 12 is configured to display "icons 18" or another "graphical element 18," EX1007, ¶30, and text. EX1007, ¶¶31, 43.

137. In my opinion, a POSITA would have found it obvious for either or both of the Rogers and Rosenberg touchscreen displays to display a first image and first descriptive text associated with the first registering mode (finger pad registering mode) and a second image and second descriptive text associated with the second registering mode (fingertip/end registering mode). One easily recognized benefit of so including such images and descriptions would be to inform the user how to move through the processes to achieve accurate and

repeatable results (e.g., biometric readings). In fact, Rogers explicitly discloses using both text and a symbol (“image”) so that the “user may have an increased authentication rate.” EX1006, 8:10-12. According to Rogers, “the electronic device 70 can provide the user with a starting point or ending point for the graphical passcode. For example, the electronic device 70 may display an ‘X’ or *target symbol* at the start position or end position of the graphical passcode.” EX1006, 8:1-5. “This may tend to decrease the authentication failure rate and help the user to more accurately render the graphical passcode in embodiments where template graphical passcode data includes plots of measured pressure and/or speed is plotted against position.” EX1006, 8:5-9.

138. A POSITA in my opinion would have understood that Rogers text and symbols would be used for both fingertip and finger pad operations such as those described in limitation [1f] and rendered obvious by Rogers and Rosenberg as both techniques would benefit from the same modifications in order to achieve increased authentication rates. Moreover, it would have been obvious to try as text and symbols are one of a few design choices for providing guidance and instructions for both forms of input. In my opinion, a POSITA would have had a reasonable expectation of success implementing these features on the Rogers-Rosenberg device because Rogers already had the technology to do so and was

already using text and symbols for its embodiments. It is my understanding that these are all proper rationale for an obviousness determination.

F. Claim 6 “The information processing apparatus according to claim 1, wherein the touch panel includes one or more capacitive sensors, such that the contact of the finger is detected based on variations in capacitance of the one or more capacitive sensors in response to the contact.”

139. The Rogers-Rosenberg combination renders claim 1 obvious. §X.B. Moreover, it is my opinion that Rogers discloses the additional requirements of Claim 6. For example, Rogers discloses that “the various embodiment methods and systems may be implemented with a variety of touch screen or touchpad technologies, including . . . *capacitive touch screens*.” EX1006, 1:66-2:2. With respect to FIG. 1, Rogers discloses that “touch screen display 40 can be any type of touch screen, such as . . . capacitive- sensing touchscreen.” EX1006, 5:6-11.

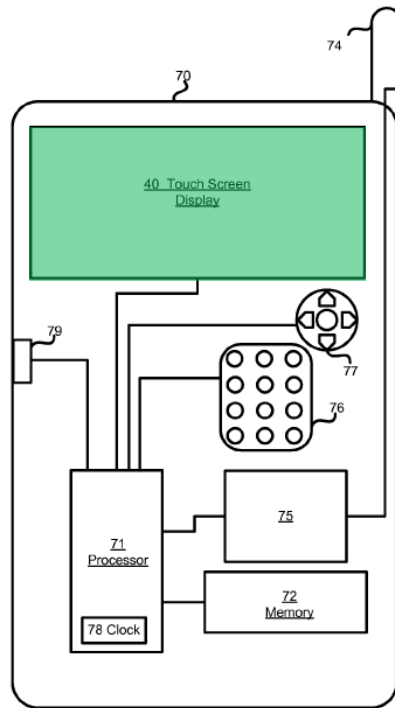


Fig. 1

EX1006, FIG. 1.

140. Rogers discloses that the contact of the finger is detected based on variations in capacitance of the one or more capacitive sensors in response to the contact: “a capacitive touch screen which is coated with a material that conducts a continuous electrical current across the sensor. When the *sensor’s ‘normal’ capacitance field (its reference state) is altered by another capacitance field, i.e., someone’s finger, electronic circuits located at each corner of the panel measure the resultant ‘distortion’ in the sine wave characteristics of the reference field and send the information about the event to the controller for mathematical processing.*” EX1006, 13:51-59.

G. Claim 7 “The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display information during the identification mode that informs the user to use a finger to execute an unlock operation of the information processing apparatus.”

141. The Rogers-Rosenberg combination renders claim 1 obvious as discussed above. §X.B. Moreover, as also discussed above, Rogers discloses its touch panel comprising a display screen configured to display information, §X.E. Rogers also discloses displaying information during the identification mode that informs the user to use a finger to execute an unlock operation of the information processing apparatus as required by Claim 7.

142. For example, during the “authenticating a graphical passcode” process of FIG. 5 (identification mode), which is used to unlock and provide access to the Rogers device, §X.D, Rogers discloses that “electronic device 7 (sp. 70) via the processor 71 and display 40 *prompts the user to input a graphical passcode that is being used as an authentication credential, step 203.*” EX1006, 9:31-36; FIG. 5:

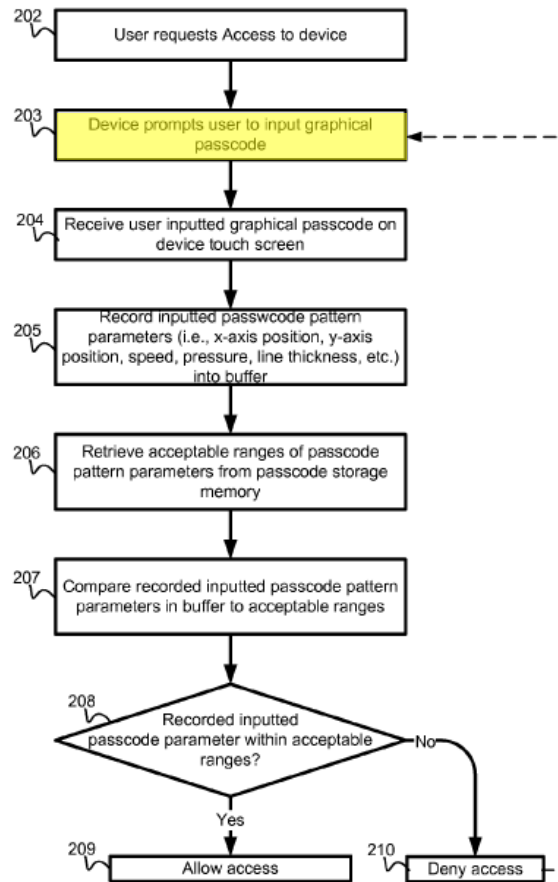


Fig. 5

XI. GROUND 2: THE COMBINATION OF ROGERS, ROSENBERG, AND MIYAZAWA RENDERS CHALLENGED CLAIMS 9-14 OBVIOUS

A. Motivation to Combine with Rosenberg and Miyazawa

143. In my opinion, as discussed above, Rogers, alone or in combination with Rosenberg, discloses touch operations that the user executes on the touch surface to create/enter the graphical passcode including multiple types of touch with different input parameters. As Rogers explains, the method “uses touches and movements on a touch sensitive surface to determine graphical passcode that are used in a manner similar to passwords. *Graphical passcodes comprise various*

combinations of swipes, taps or drags on a touchscreen surface as defined by a user. A user's selected graphical passcode is stored in memory for comparison to subsequent entries of graphical passcode in order to authenticate the users."

EX1006, Abstract. In other words, the graphical passcode disclosed by Rogers, alone or in combination with Rosenberg, "is essentially a *series of touches, swipes, and/or taps on a touchsurface of varying pressure, speed and position.*" EX1006, at 3:34-36. The user registers or re-enters the graphical passcode by performing various types of touches on the disclosed touch surface, *i.e.*, "by touching a touchsurface in a series of movements and touches within a brief period of time." EX1006, 3:60-62.

144. In my opinion, a POSITA would have found it obvious and been motivated to integrate the gestures disclosed by Miyazawa into, among other things, Rogers' graphical passcode for registration and entry. A POSITA would have been motivated to combine the teachings of Rogers-Rosenberg and Miyazawa because the references share the same field of touch input technology including touch surfaces, especially including touch input devices that display information, which makes them analogous art to the '086 patent. For example, the Miyazawa disclosures "relates to an information processing apparatus, an input operation determination method, and an input operation determination program and is suitable for an information processing apparatus including, for example, a touch

panel.” EX1008, 1:9-13. And Miyazawa discloses that “[t]he touch screen 102 includes a liquid crystal panel 102A which is a display device displaying various kinds of information and a touch panel 102B which is an input operation device receiving an input operation.” EX1008, 5:25-36. Similarly, Rogers discloses “[a] method or system for electronic access security [that] uses touches and movements on a touch sensitive surface to determine graphical passcode that are used in a manner similar to passwords.” EX1006, Abstract. Additionally, as explained immediately above, all three references disclose touch detection units that recognize different types of touch operations and their detection.

145. A POSITA in my opinion therefore would have considered the “touch,” “swipe,” and “tap” operations disclosed in Rogers-Rosenberg and been motivated to modify that apparatus to support the “dragging,” “flicking,” “tapping,” and “pinching” operations disclosed in Miyazawa. Further, the gesture operations in Rogers and Miyazawa are identical to the gesture operations disclosed in the ’086 patent, EX1001, 3:46-56 (“Among types of operations performed by the user on the portable terminal 0 are tapping, dragging, flicking, and pinching. Tapping is an operation which the user touches one point of the screen with a finger for a moment on the touch panel 1. Dragging is an operation which the user moves his or her finger over the screen of the touch panel 1 while the finger is in contact therewith. Flicking is an operation which the user quickly

slides his or her finger on the screen of the touch panel 1 while touching it.

Pinching is an operation which the user touches two points of the screen of the touch panel 1 with two fingers and changes the distance between the two panels.”).

In my opinion, a POSITA would have found this modification to be a simple substitution of elements well known in the art and would have had a reasonable expectation of success in achieving the benefits disclosed in all three references by making the modification. It is my understanding that these are all proper rationale for an obviousness determination.

B. Claim 9 “The information processing apparatus according to claim 1, wherein the first controller is configured to execute one or more of tapping, dragging, flicking, and pinching operations based on the detection of contact of the finger.”

146. The Rogers-Rosenberg combination renders claim 1 obvious as discussed above. §X.B. Rogers also discloses the claimed “first controller,” §X.B.4. Rogers renders obvious, alone or in combination with Miyazawa, that “the first controller is configured to execute one or more of tapping, dragging, flicking, and pinching operations based on the detection of contact of the finger” as required by Claim 9.

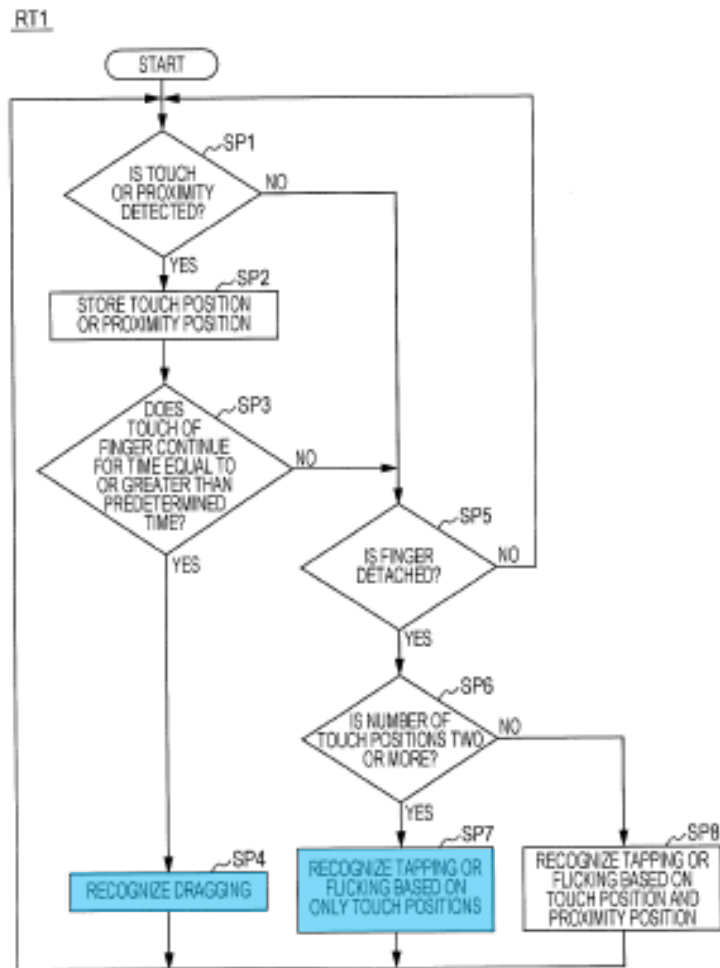
147. For example, Rogers discloses a “method and system for electronic access security uses touches and movements on a touch sensitive surface to determine graphical passcode that are used in a manner similar to passwords. Graphical passcodes comprise various combinations of swipes, *taps* or drags on a

touchscreen surface as defined by a user. A user's selected graphical passcode is stored in memory for comparison to subsequent entries of graphical passcode in order to authenticate the users." EX1006, Abstract. "The graphical passcode is essentially a series of touches, swipes, and/or *taps* on a touchsurface of varying pressure, speed and position." EX1006, 3:34-36. Fig. 2A of Rogers "illustrates an exemplary graphical passcode consisting of a tap, a swipe, and two taps." EX1006, 2:20-21.

148. The entered graphical passcode is used e.g., in an authentication process. EX1006, FIG. 5. It is my opinion that a POSITA would have understood that Rogers first controller would be configured to execute the tapping operation based on the detection of contact of the finger based on these disclosures.

149. To the extent Patent Owner argues that this limitation also requires dragging, flicking, and/or pinching operations, Miyazawa discloses these operations. Specifically, Miyazawa at FIG 11 shows an operation recognition processing order with steps SP4, SP7 to execute dragging, tapping, and flicking operations:

FIG. 11



EX1008, FIG. 11.

150. Miyazawa also discloses the detection of “pinch-in or pinch-out” touch operations: “Moreover, the CPU 110 recognizes whether two fingers are moved in a direction in which the two fingers are closer to each other on the surface parallel to the operation surface or in a direction in which the two fingers are distant from each other, *based on the touch position* and the proximity position,

and determines whether the pinch-in is performed or the pinch-out is performed.”

EX1008, 15:44-56.

C. Claim 10 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute tapping operations, and the tapping operations include detection of contact of the finger for a first time period.”

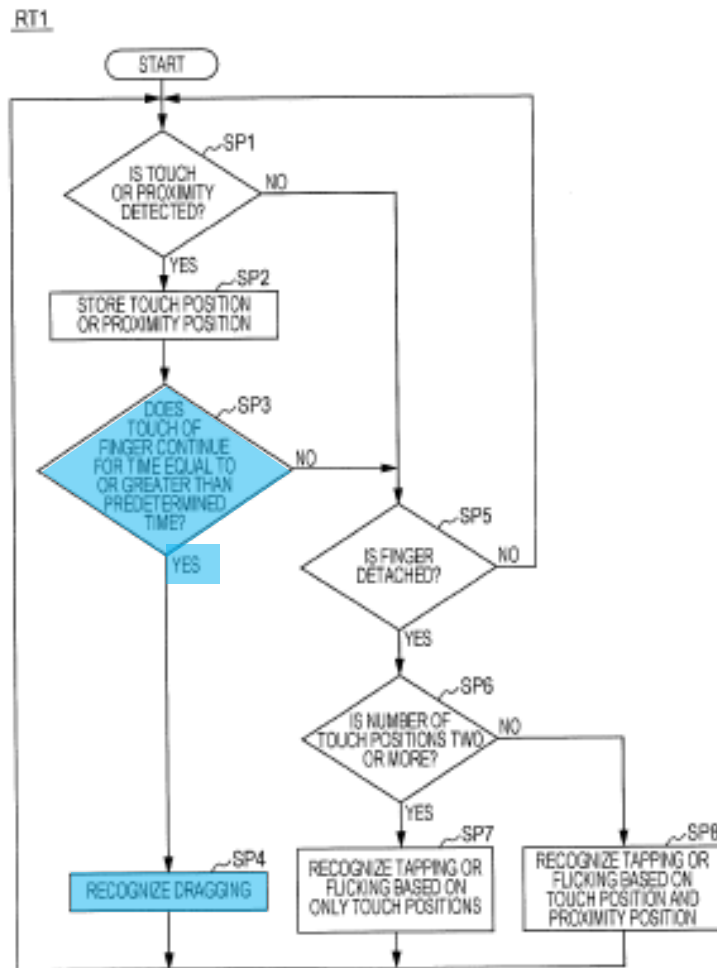
151. The Rogers-Rosenberg-Miyazawa combination renders claim 9 obvious as discussed above. §XI.B. As also discussed above, Rogers alone or in view of Miyazawa renders obvious that the first controller is configured to execute tapping operations. §XI.B. Moreover, Roger renders obvious that the tapping operations include detection of contact of the finger for a first time period required by Claim 10. Specifically, Rogers requires the user to create the graphical passcode “by touching a touchsurface in a series of movements and touches *within a brief period of time.*” EX1006, 3:60-62. Rogers also discloses that graphical passcode parameters “may be enveloped against time For authentication, a graphical passcode must occupy a portion of an envelope.” EX1006, 3:52-56.

152. Rogers further discloses that “when the template graphical passcode is inputted, one or more measurable parameters (e.g. *timing...*) of the inputted template graphical passcode is measured by the touchsurface. The measured parameters may be plotted as a function of time and/or position on the touchsurface.” EX1006, 4:15-21.

D. Claim 11 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period.”

153. The Rogers-Rosenberg-Miyazawa combination renders claim 9 obvious as discussed above. §XI.B. Additionally, Rogers alone or in view of Miyazawa disclose or render obvious that the first controller is configured to execute tapping operations. §XI.B. Moreover, Miyazawa at FIG 11 “recognize[s] dragging” when it is determined that the “touch of finger continue[s] for time equal to or greater than predetermined time” as required by Claim 11. EX1008, FIG. 11 (YES at SP3 leading to SP4).

FIG. 11



EX1008, FIG. 11.

154. Miyazawa states:

In step SP3, the CPU 110 determines whether the touch of the finger continues for a time equal to or longer than a predetermined time based on the history data. When the positive result is obtained in step SP3, it means that the operation surface is continuously touched with the finger, and then the CPU 110 allows the process

to proceed to step SP4 subsequent to step SP3. In step SP4, the CPU 110 determines that the operation input on the touch panel 102B is dragging, thus recognizes that the dragging is performed, and thus performs the process corresponding to the dragging.

EX1008, 10:59-11:15, *see also* 7:33-37 (“When detecting that the *touch of the finger on the operation surface continues for a time equal to or longer than a predetermined time* based on the history data, the CPU 110 recognizes an operation of continuously touching the finger on the operation surface, that is, *the dragging and thus recognizes the dragging as an input operation.*”).

E. Claim 12

1. **[12a] “The information processing apparatus according to claim 9, wherein the first controller is configured to execute flicking operations, and the flicking operations correspond to the user sliding the finger for a first time period, and”**

155. The Rogers-Rosenberg-Miyazawa combination renders claim 9 obvious as discussed above. §XI.B. As also discussed above, Rogers in view of Miyazawa renders obvious that the first controller is configured to execute flicking operations. §XI.B. It is also my opinion that Rogers or Miyazawa renders obvious that that flicking operations correspond to the user sliding the finger for a first time period as required by limitation [12a]. For example, Rogers FIG. 2E illustrates a swipe 22 in the form of a trapezoid shape where the speed of the swipe 22 is initially fast but slows down over time, thus showing the user sliding the finger for

a first time period. EX1006, 6:14-19. A POSITA would have understood that a short swipe (i.e., over a short period of time) with a user's fingertip is a flick operation.

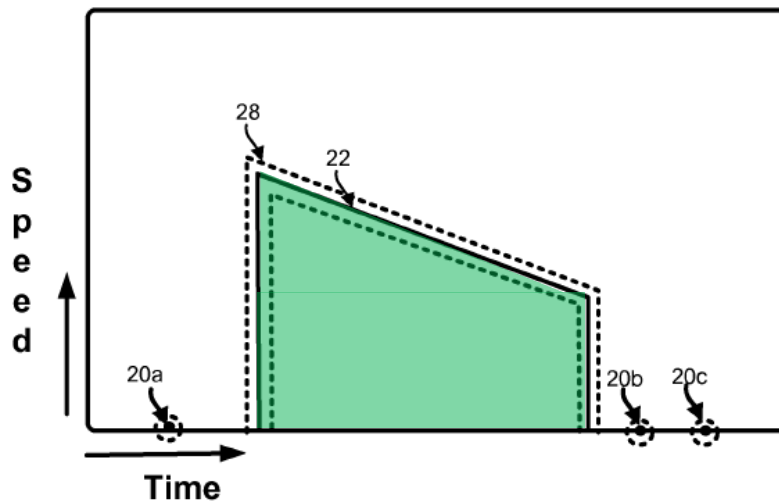


Fig. 2E

156. Additionally, Miyazawa discloses that “CPU 110 detects the *movement* of the touch position and determines that the performed input operation is *flicking*, when the distance between the start touch position and the end touch position is equal to or greater than a predetermined value.... The predetermined value is a value in which it is considered that the touch position is barely moved.” EX1008, 7:54-63. Moreover, Miyazawa identifies a dragging operation based on a determination of whether the user's touch “continue[s] for time *equal to or greater* than predetermined time,” EX1008, FIG. 11 (YES at SP3 leading to SP4), but determines flicking when the contact is less than that predetermined time (NO at step SP3 leading to SP7).

FIG. 11

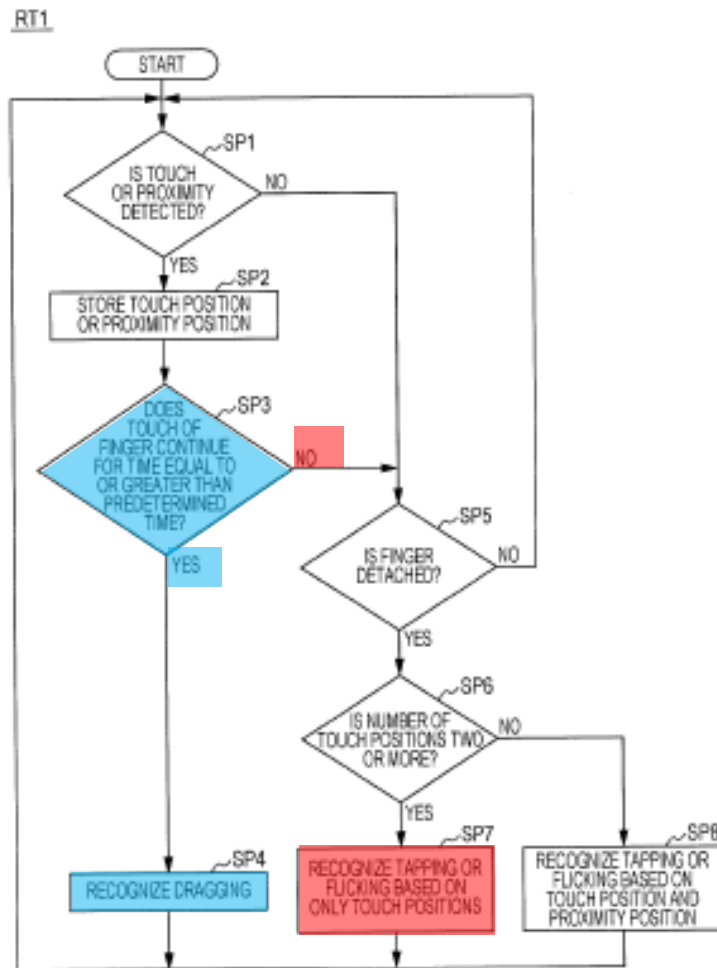


FIG. 1008, FIG. 11.

2. [12b] “wherein the first controller is configured to execute pinching operations, and the pinching operations correspond to the user establishing two contacts and increasing the distance between the established two contacts.”

157. As discussed above, Rogers in view of Miyazawa renders obvious that the first controller is configured to execute pinching operations. §XI.B. Miyazawa further discloses a pinching operation that maps to the user establishing two

contacts on the touchscreen and then increasing the distance between the established two contacts (while maintaining contact with the touchscreen) as required by limitation [12b]. Specifically, Miyazawa discloses that “CPU 110 recognizes whether *two fingers are moved on the surface* parallel to the operation surface based on both the touch position and the proximity position detected after the touch of the finger, and *determines whether ... pinch-in or pinch-out is performed.*” EX1008, 15:44-49. Moreover, the CPU 110 recognizes whether *two fingers are moved* in a direction in which the two fingers are closer to each other on the surface parallel to the operation surface or *in a direction in which the two fingers are distant from each other*, ... and determines whether the pinch-in is performed or the pinch-out is performed.” EX1008, 15:50-56.

F. Claim 13

1. **[13a] The information processing apparatus according to claim 9, wherein the first controller is configured to execute said dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period, and**

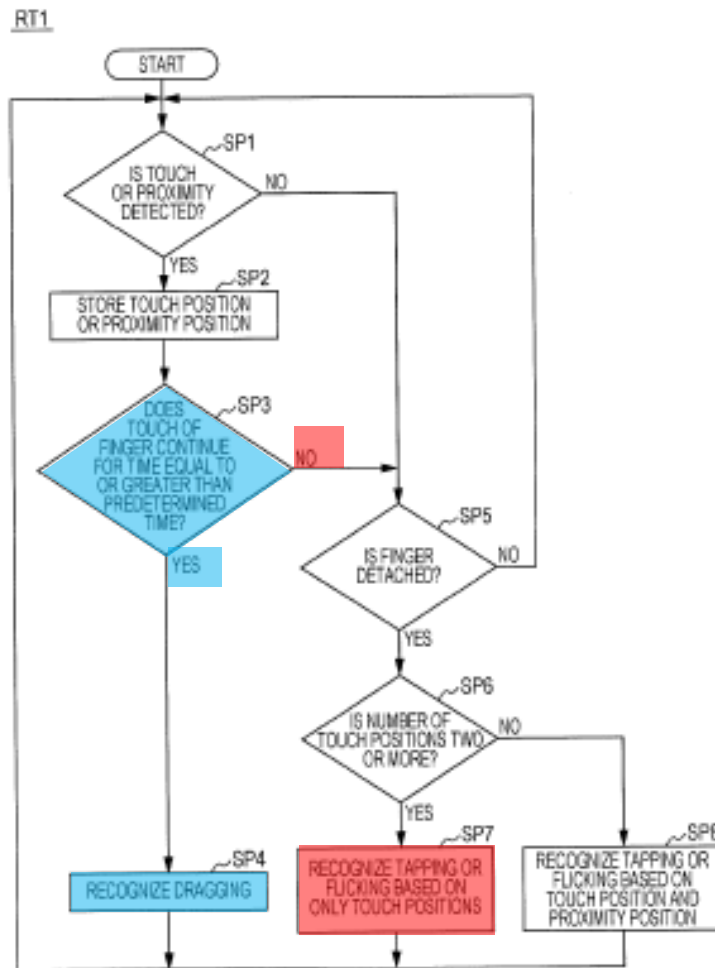
158. The Rogers-Rosenberg-Miyazawa combination renders claim 9 obvious, as discussed above. §XI.B. Moreover, as also discussed above, Miyazawa discloses or renders obvious that the first controller is configured to execute dragging operations that correspond to the user moving the finger while maintaining contact for a first time period. §XI.D.

2. **[13b] wherein the first controller is configured to execute said flicking operations, and the flicking operations correspond to the user sliding the finger for a second time period that is shorter than the first time period.**

159. Moreover, Rogers or Miyazawa render obvious that the first controller is configured to execute flicking operations that correspond to the user moving the finger while maintaining contact for a time period as required by limitation [13b].

§XI.E.1. In my opinion, a POSITA would have understood from the teachings of Rogers and Miyazawa that a “flicking operation” would require the user’s sliding contact to be over a shorter period of time than the period of time required for a dragging operation. Miyazawa satisfies this requirement by disclosing evaluating its dragging operation based on a determination of whether the user’s touch “continue[s] for time equal to or *greater* than predetermined time,” EX1008, FIG. 11 (YES at SP3 leading to SP4), but determining flicking when the contact is less than that predetermined time (NO at step SP3 leading to SP7).

FIG. 11



EX1008, FIG. 11.

G. Claim 14. The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen displaying a plurality of icons corresponding to applications being executed on the information processing apparatus, and the information processing apparatus is configured to execute an operation for moving at least one of the plurality of icons based on an operation that requires contact by a finger for a predetermined period of time.

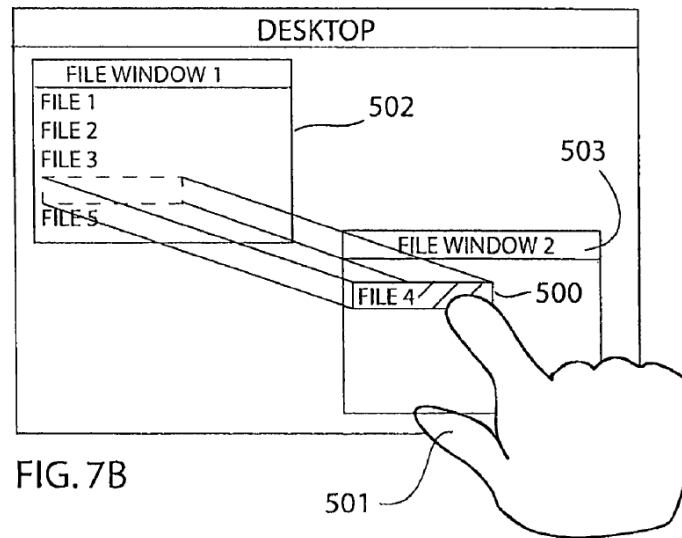
160. The Rogers-Rosenberg combination renders claim 1 obvious as discussed above. §X.B. Moreover, and as also discussed above, Rogers and

Rosenberg both disclose a touch panel comprising a display screen configured to display information, §X.E. In my opinion, Miyazawa renders the rest of the requirements of Claim 14 obvious.

161. For example, Miyazawa discloses or renders obvious that the first controller is configured to execute dragging operations that correspond to the user moving the finger while maintaining contact for a first time period. §XI.D. A POSITA would have understood that one function of a dragging operation is to move objects displayed on the touchscreen (often referred to as a “drag and drop operation”). Indeed, this function was well known by at least 2007 as illustrated by the disclosures of Westerman:

Drag-and-drop function can be invoked by touching, with at least one finger, the image associated with the object to be dropped and graphically dragging the object to the desired drop location by maintaining the touch, such as shown in FIG. 7B, illustrating a drag and drop of a file listing 501 from folder window 502 to folder window 503.

EX1009, 12:41-46; FIG. 7B.



EX1009, FIG. 7B.

162. A POSITA would have also understood that the object that can be dragged and drop includes icons, such as those used to represent applications installed on/accessible by the apparatus as this was within the POSITA's knowledge as evidenced by Westerman's disclosures:

The display device 68 can be configured to display a graphical user interface (GUI) 69 that can provide an easy to use interface between a user of the computer system and the operating system or application running thereon. Generally speaking, *the GUI 69 can represent programs, files and operational options with graphical images, objects, or vector representations.* The graphical images can include windows, fields, dialog boxes, menus, *icons*, buttons, cursors, scroll bars, etc. Such images can be arranged in predefined

layouts, *or can be created dynamically to serve the specific actions being taken by a user.* During operation, *the user can select and/or activate various graphical images* in order to initiate functions and tasks associated therewith.

EX1009, 5:20-32.

163. A POSITA would have also understood that “a plurality of icons corresponding to applications being executed on the information processing apparatus” would have been displayed and capable of being dragged and dropped. For instance, Westerman discloses that “gestures 85 can be identified as commands for performing actions in *applications* stored in the memory 58, modifying *image objects* shown on the display 68.” EX1009, 6:45-47.

XII. GROUND 3: THE COMBINATION OF ROGERS AND REKIMOTO RENDERS CHALLENGED CLAIMS 1, 2 AND 4-7 OBVIOUS

A. Motivation to Combine Rogers with Rekimoto

164. In my opinion, it would have been obvious to a POSITA to combine the teachings of Rogers and Rekimoto because both references share the same field of inputting information via touchsurface technology, which makes them analogous art to the '086 patent. EX1006, Abstract, FIGS. 1, 2A; EX1010, Abstract, FIG. 1. Additionally, Rekimoto discloses its fingertip and finger pad touches as a solution to provide “continuous and smooth operation,” which was a

problem with certain operations at the time, EX1010, 1:53-67, and a POSITA would have understood that this would have added a benefit to Rogers' device.

165. Thus, in my opinion a POSITA would have found the combination obvious to try due to the similarity of the technical teachings of the art, and also because a POSITA would have recognized that Rekimoto's disclosures, applied to Rogers, would facilitate "continuous and smooth operation" for certain touch functions in Rogers. A POSITA therefore would have been motivated to look at Rekimoto to improve Rogers, and vice-versa.

166. Further, it is my opinion that a POSITA would have recognized that the disclosure in Rogers of distinguishing between a "larger fingertip and a small stylus tip" based on "area difference[s]" between the two input types would have been better accomplished through Rekimoto's disclosure of its fingertip and finger pad distinction technique. Specifically, Rekimoto discloses:

During the input operation, the contact area of the contact sensor section 2 occupied by the fingertip equals a small area S1... The contact area of the contact sensor section 2 touched by the finger pad equals a large area S2... That is, compared with the area S1, which is an area of the contact sensor section 2 surface touched by the fingertip, the area S2 touched by the finger pad is larger

(wider). *These areas S1, S2 can be clearly distinguished by using a threshold St of a specified area as a boundary.*

EX1010, 5:18-31.

167. A POSITA therefore would have considered the disclosures in Rekimoto and been motivated to modify Rogers' "larger fingertip and a small stylus tip" example so that it instead used the finger pad versus fingertip distinction disclosed by Rekimoto. A POSITA in my opinion would have found this modification to be a simple substitution of elements well known in the art, and would have had a reasonable expectation of success in achieving the benefits disclosed in Rekimoto by making the modification, which involved only routine skill.

168. Moreover, adding Rekimoto's fingertip and finger pad touch detection to Rogers would simply involve applying a known technique (i.e., fingertip and finger pad touch detection/distinction as taught by Rekimoto) to a known device ready for improvement (Roger's apparatus having larger fingertip and a small stylus tip capabilities) to yield predictable results (simple to use touch screen interface with multipoint targeting and multi-finger gesturing).

169. In my opinion, it also would have been obvious to combine Rogers with Rekimoto because both references disclose touch screen interfaces that detect a contact area of a finger. Rogers discloses that the "measurable parameters" of a

“template graphical passcode” can include “contact area.” EX1006, 4:15-19.

Rekimoto teaches distinguishing between finger pad and fingertip touches by touch “areas S1, S2 [that] can be clearly distinguished by using a threshold St of a specified area as a boundary size, shape, and/or orientation of the detected finger.” EX1010, 5:29-31. Rekimoto further discloses that when compared to the fingertip contact S1, “the area S2 touched by the finger pad is larger (wider).” EX1010, 5:26-291. A POSITA would have viewed these disclosures in Rosenberg and been motivated to modify the “graphical passcode” features of Rogers so that the disclosed device detected information input by a finger pad or fingertip, because it would provide a “clearly distinguish[able]” basis upon which to program the device disclosed in Rogers to detect a “measurable parameter” based on “contact area.”

170. A POSITA in my opinion would have further recognized that these features of Rogers and Rekimoto could be combined because the fingertip and finger pad are distinguishable inputs for a user, and because Rekimoto teaches the ability to “clearly distinguish[.]” between the two, it would have been obvious to modify Rogers (to the extent not already taught) to receive input information including a pad or tip of the finger. Because Rogers also teaches the contact area on the touchscreen may be one of the parameters for the graphical passcode, Rogers expressly suggests to a POSITA the ease of making the modification to

detect the tip/pad of the finger and that the area of contact is a desirable parameter for inputting an authentication passcode. In my opinion, a POSITA would have had a reasonable expectation of success of modifying Rogers in this manner for at least the same reasons. It is my understanding that these are all proper rationale for an obviousness determination.

B. Claim 1

1. [1pre] An information processing apparatus comprising:

171. To the extent the preamble is limiting, Rogers discloses it. §X.B.1.

2. [1a] a touch panel configured to detect a contact of a finger of a user;

172. Rogers discloses this limitation. §X.B.2.

3. [1b] a detector configured to detect first information necessary for an identification of the user when the contact is detected between the touch panel and the finger of the user;

173. Rogers discloses this limitation. §X.B.2.

4. [1c] a first controller configured to control the information processing apparatus to operate into two operating modes: at least an identification mode and a registering mode, as the operating mode thereof;

174. Rogers discloses this limitation. §X.B.3.

5. [1d] memory that is configured to store second information relating to the identification of the user, which is stored in advance; and

175. Rogers discloses this limitation. §X.B.5.

6. **[1e] a second controller configured to execute a specified process when said first information and said second information are coincident within said identification mode, wherein:**

176. Rogers discloses this limitation. §X.B.6.

7. **[1f] in said registering mode, there are provided a first registering mode for inputting input information by a pad of the finger, and a second registering mode for inputting input information by an end of the finger, and said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode.**

177. In my opinion, the Rogers-Rekimoto combination renders this limitation obvious. As shown above in Ground 1, it is also my opinion that Rogers alone renders obvious a registering mode providing a first registering mode for inputting input information by a pad of the finger, and a second registering mode for inputting input information by an end of the finger, and said second information relating to the identification of the user is produced upon basis of the input information, which is inputted at least in the first or second mode. §X.B.7.

Rogers in view of Rekimoto

178. To the extent Patent Owner argues that Rogers does not fully disclose limitation [1f] because Rogers does not explicitly recite the use of finger pad and fingertip inputs, it is my opinion that Rogers in view of Rekimoto renders this limitation obvious.

179. Rekimoto discloses inputting input information by a pad of the finger (“finger pad”) and inputting input information by an end of the finger (“fingertip”):

FIGS. 2A and 2B are a schematic sectional view and a plan view both showing the control panel (the surface of the contact sensor section 2) of an input section of the input device 1 which a user presses by erecting a finger and thus with a *fingertip*.... FIGS. 3A and 3B are a schematic sectional view and a plan view both showing the control panel (the surface of the contact sensor section 2) of the input device 1 which the user presses by laying down the finger and thus with the *finger pad*....

EX1010, 5:13-24.

FIG.2A

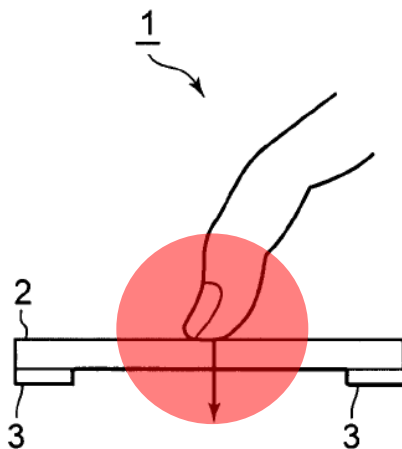
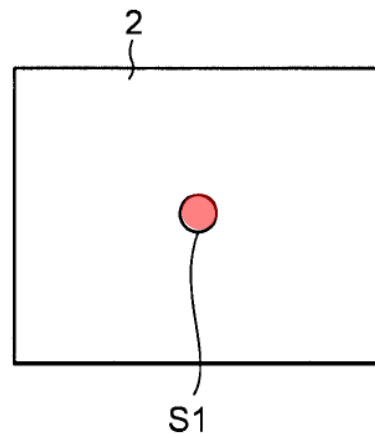


FIG.2B



EX1010, FIGS. 2A, 2B.

FIG.3A

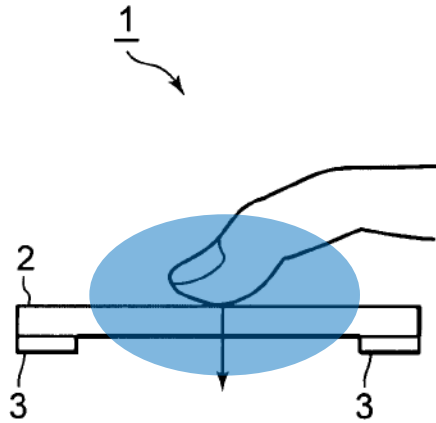
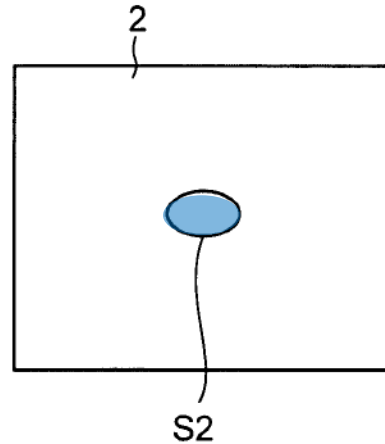


FIG.3B

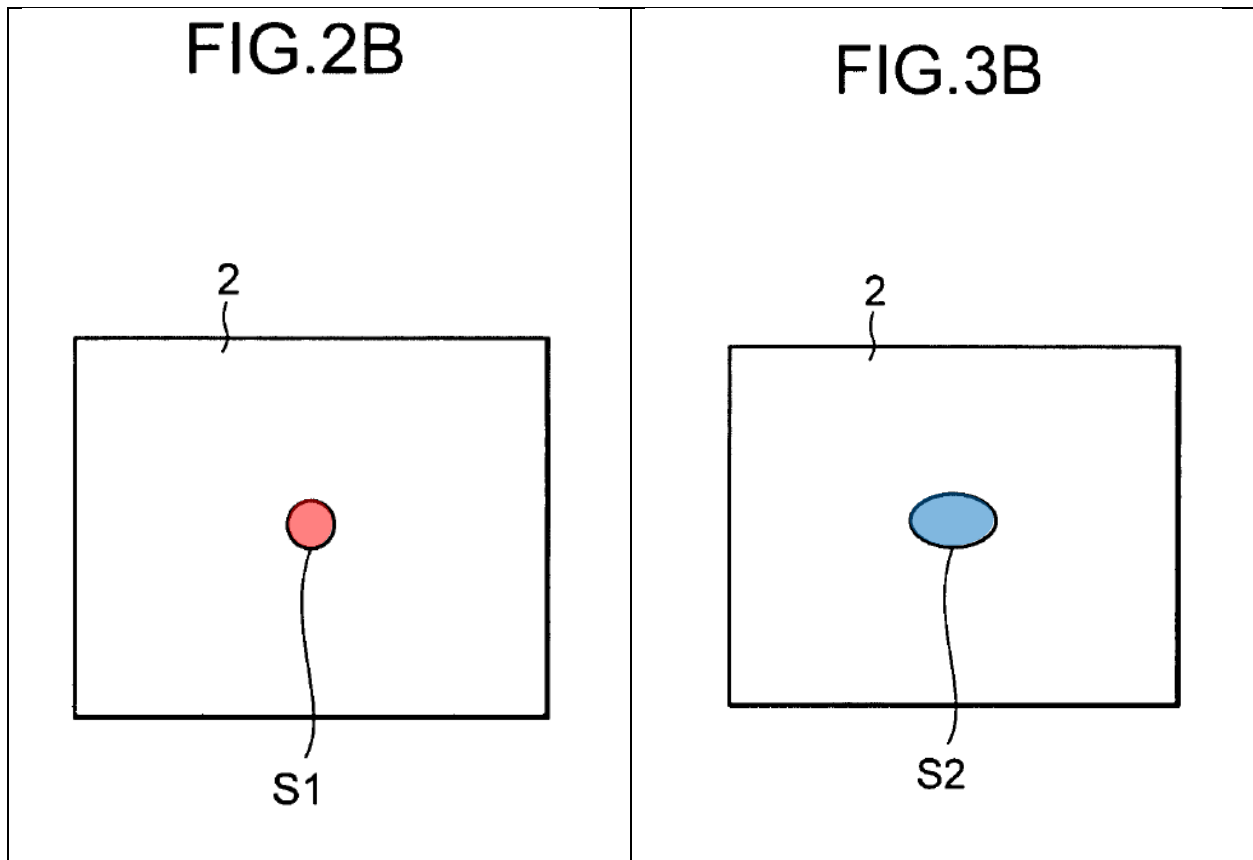


EX1010, FIGS. 3A, 3B.

180. Rekimoto explicitly discloses distinguishing fingertip touches and finger pad touches:

During the input operation, the *contact area of the contact sensor section 2 occupied by the fingertip equals a small area S1...* The contact area of the contact sensor section 2 touched by the *finger pad equals a large area S2...* That is, compared with the area S1, which is an area of the contact sensor section 2 surface touched by the fingertip, the area S2 touched by the finger pad is larger (wider). *These areas S1, S2 can be clearly distinguished by using a threshold St of a specified area as a boundary.*

EX1010, 5:18-31.



181. Rekimoto discloses that fingertip and finger pad touches can be used for different processing (zoom operations in the illustrated example): “Therefore, by pressing the input device 1 by erecting a finger and thus with a fingertip, the user can perform first processing for zooming in on an image in response to the pressing force. Similarly, by pressing the input device 1 by laying the finger down and thus with the finger pad, the user can perform second processing for zooming out on the image in response to the pressing force.” EX1010, 5:31-37.

- C. Claim 2. The information processing apparatus according to claim 1, wherein said first information includes a position and an area of the finger contacting with said touch panel.**

182. The Rogers-Rekimoto combination renders claim 1 obvious. §XII.B.

Rogers further discloses this limitation. §X.C.

- D. Claim 4. The information processing apparatus according to claim 1, wherein said specified process includes releasing of a lock of resting an operation of said information processing apparatus.**

183. The Rogers-Rekimoto combination renders claim 1 obvious. §XII.B.

Rogers further discloses or renders obvious this limitation. §X.D.

- E. Claim 5. The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display a first image and first descriptive text associated with the first registering mode and a second image and second descriptive text associated with the second registering mode.**

184. The Rogers-Rekimoto combination renders claim 1 obvious. §XII.B.

In my opinion, Rogers in view of Rekimoto renders obvious the inputting of second information relating to the identification of the user in the first or second registering mode, §XII.B.7, and renders obvious this limitation. For example, Rogers discloses that its touch panel 40 includes a display. EX1006, 3:4-5 (“As used herein, a ‘touchscreen’ is a touch input device with an associated image display.”), 5:6-16:

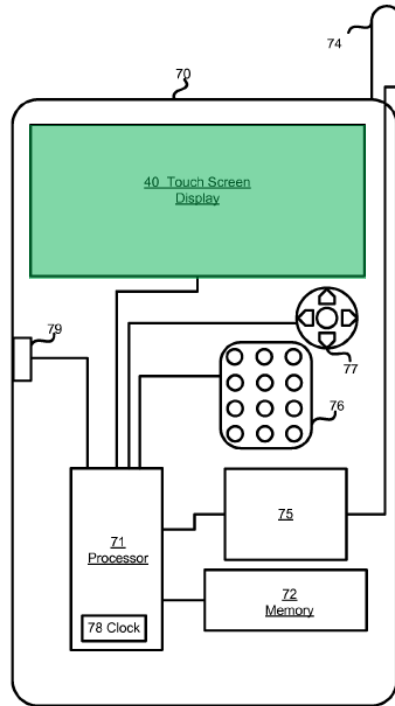


Fig. 1

EX1006, FIG. 1.

185. Rekimoto also discloses a touch display and manipulating displayed objects:

FIG. 5A

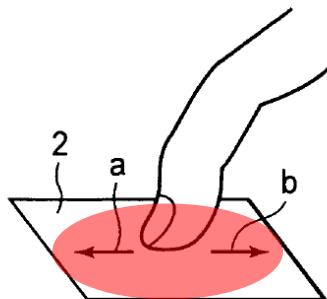


FIG. 5B



EX1010, FIGS. 5A, 5B. Rekimoto's display is configured to display "function names, icons representing functions, or the like." EX1010, 9:40-43.

186. It is my opinion that a POSITA would have found it obvious for the Rogers and/or Rekimoto touchscreen displays to display a first image and first descriptive text associated with the first registering mode (finger pad registering mode) and a second image and second descriptive text associated with the second registering mode (finger tip/end registering mode). One benefit of doing so would be to help/guide the user through the processes to achieve accurate and repeatable results. Indeed, Rogers explicitly discloses using both text and a symbol (image) so that the "user may have an increased authentication rate." EX1006, 8:10-12.

According to Rogers, "the electronic device 70 can provide the user with a starting point or ending point for the graphical passcode. For example, the electronic device 70 may display an '*X*' or *target symbol* at the start position or end position of the graphical passcode." EX1006, 8:1-5. "This may tend to decrease the authentication failure rate and help the user to more accurately render the graphical passcode in embodiments where template graphical passcode data includes plots of measured pressure and/or speed is plotted against position." EX1006, 8:5-9.

187. A POSITA would have understood that Rogers text and symbols would be used for both fingertip and finger pad operations such as those described in limitation [1f] and rendered obvious by Rogers and Rekimoto as both techniques

would achieve the same benefits (e.g., increased authentication rate). Moreover, it would have been obvious to try as one of a few design choices (use of text and symbol guidance versus no guidance) for both forms of input. A POSITA in my opinion would have had a reasonable expectation of success implementing these features on the Rogers-Rekimoto device because Rogers already had the technology to do so and was already doing so for its embodiments. It is my understanding that these are all proper rationale for an obviousness determination.

F. Claim 6. The information processing apparatus according to claim 1, wherein the touch panel includes one or more capacitive sensors, such that the contact of the finger is detected based on variations in capacitance of the one or more capacitive sensors in response to the contact.

188. The Rogers-Rekimoto combination renders claim 1 obvious. §XIII.B.
Rogers further discloses this limitation. §X.F.

G. Claim 7. The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen configured to display information during the identification mode that informs the user to use a finger to execute an unlock operation of the information processing apparatus.

189. The Rogers-Rekimoto combination renders claim 1 obvious. §XII.B.
Rogers further discloses this limitation. §X.G.

XIII. GROUND 4: THE COMBINATION OF ROGERS, REKIMOTO AND MIYAZAWA RENDERS CHALLENGED CLAIMS 9-14 OBVIOUS

A. Motivation to Combine Rogers with Rekimoto and Miyazawa

190. In my opinion, it would have been obvious to a POSITA to combine the Rogers-Rekimoto apparatus with Miyazawa and a POSITA would have been motivated and capable of doing so for at least the same reasons provided for combining Rogers-Rosenberg with Miyazawa. §XI.A.

191. For example, Rogers, alone or in combination with Rekimoto, discloses various touch operations that the user executes on the touch surface to create/enter the graphical passcode. The method “uses touches and movements on a touch sensitive surface to determine graphical passcode that are used in a manner similar to passwords. *Graphical passcodes comprise various combinations of swipes, taps or drags on a touchscreen surface as defined by a user.* A user’s selected graphical passcode is stored in memory for comparison to subsequent entries of graphical passcode in order to authenticate the users.” EX1006, Abstract. In other words, the graphical passcode disclosed by Rogers, alone or in combination with Rekimoto “is essentially a *series of touches, swipes, and/or taps on a touchsurface of varying pressure, speed and position.*” EX1006, at 3:34-36. The user creates the graphical passcode by executing touch operations on the disclosed touch surface, *i.e.*, “by touching a touchsurface in a series of movements and touches within a brief period of time.” EX1006, 3:60-62.

192. It is my opinion that a POSITA would have been motivated to incorporate the gestures disclosed by Miyazawa for e.g., the creation/entry of Rogers' graphical passcode. A POSITA in my opinion would have been motivated to combine the teachings of Rogers-Rekimoto and Miyazawa because the references share the same field of touchsurface and touch input technology, particularly touch input devices capable of displaying information, which makes them analogous art to the '086 patent. The invention disclosed by Miyazawa "relates to an information processing apparatus, an input operation determination method, and an input operation determination program and is suitable for an information processing apparatus including, for example, a touch panel." EX1008, 1:9-13. And Miyazawa discloses that "[t]he touch screen 102 includes a liquid crystal panel 102A which is a display device displaying various kinds of information and a touch panel 102B which is an input operation device receiving an input operation." EX1008, 5:25-36. Similarly, Rogers discloses "[a] method or system for electronic access security [that] uses touches and movements on a touch sensitive surface to determine graphical passcode that are used in a manner similar to passwords." EX1006, Abstract. Additionally, all three references disclose touch detection units that recognize different types of touch operations and their detection.

193. In my opinion, a POSITA therefore would have considered the “touch,” “swipe,” and “tap” operations disclosed in Rogers-Rekimoto and been motivated to modify that apparatus to execute the “dragging,” “flicking,” “tapping,” and “pinching” operations disclosed in Miyazawa. Further, the gesture operations in Rogers and Miyazawa are identical to the gesture operations disclosed in the ’086 patent, EX1001, 3:46-56 (“Tapping is an operation which the user touches one point of the screen with a finger for a moment on the touch panel 1. Dragging is an operation which the user moves his or her finger over the screen of the touch panel 1 while the finger is in contact therewith. Flicking is an operation which the user quickly slides his or her finger on the screen of the touch panel 1 while touching it. Pinching is an operation which the user touches two points of the screen of the touch panel 1 with two fingers and changes the distance between the two panels.”). A POSITA would have found this modification to be a simple substitution of elements well known in the art and would have had a reasonable expectation of success in achieving the benefits disclosed in all three references by making the modification. It is my understanding that these are all proper rationale for an obviousness determination.

B. Claim 9 “The information processing apparatus according to claim 1, wherein the first controller is configured to execute one

or more of tapping, dragging, flicking, and pinching operations based on the detection of contact of the finger.”

194. The Rogers-Rekimoto combination renders claim 1 obvious. §XII.B.

Rogers alone or in combination with Miyazawa discloses or renders obvious this limitation. §XI.B.

C. Claim 10 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute tapping operations, and the tapping operations include detection of contact of the finger for a first time period.”

195. The Rogers-Rekimoto-Miyazawa combination renders claim 9 obvious. §XIII.B. Rogers alone or in combination with Miyazawa discloses or renders obvious this limitation. §XI.B.

D. Claim 11 “The information processing apparatus according to claim 9, wherein the first controller is configured to execute dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period.”

196. The Rogers-Rekimoto-Miyazawa combination renders claim 9 obvious. §XIII.B. Miyazawa discloses or renders obvious this limitation. §XI.B.

E. Claim 12

1. [12a] “The information processing apparatus according to claim 9, wherein the first controller is configured to execute

flicking operations, and the flicking operations correspond to the user sliding the finger for a first time period, and”

197. The Rogers-Rekimoto-Miyazawa combination renders claim 9 obvious. §XIII.B. Rogers alone or in combination with Miyazawa discloses or renders obvious this limitation. §XI.E.1.

2. **[12b] “wherein the first controller is configured to execute pinching operations, and the pinching operations correspond to the user establishing two contacts and increasing the distance between the established two contacts.”**

198. Miyazawa discloses or renders obvious this limitation. §XI.E.2.

F. Claim 13

1. **[13a] “The information processing apparatus according to claim 9, wherein the first controller is configured to execute said dragging operations, and the dragging operations correspond to the user moving the finger while maintaining contact for a first time period, and”**

199. The Rogers-Rekimoto-Miyazawa combination renders claim 9 obvious. §XIII.B. Miyazawa discloses or renders obvious this limitation. §XI.F.1.

2. **[13b] “wherein the first controller is configured to execute said flicking operations, and the flicking operations correspond to the user sliding the finger for a second time period that is shorter than the first time period.”**

200. Rogers alone or in combination with Miyazawa renders obvious this limitation. §XI.F.2.

G. Claim 14. “The information processing apparatus according to claim 1, wherein the touch panel comprises a display screen displaying a plurality of icons corresponding to applications being

executed on the information processing apparatus, and the information processing apparatus is configured to execute an operation for moving at least one of the plurality of icons based on an operation that requires contact by a finger for a predetermined period of time.”

201. The Rogers-Rekimoto combination renders claim 1 obvious. §XII.B.

Miyazawa discloses or renders obvious this limitation. §XI.G.

XIV. CONCLUSION

202. Claims 1, 2, 4-7, and 9-14 of the '086 patent are invalid for the reasons discussed above.

Exhibit A



Seth James Nielson's Vita

(512) 387-4310

seth@crimsonvista.com

March 2024

Academic Degrees

2009	Ph.D. Computer Science , Rice University, Houston, TX
2004	M.S. Computer Science , Brigham Young University, Provo, UT
2000	B.S. Computer Science , Brigham Young University, Provo, UT

Certifications

CISSP

Current Appointments

Founder and Chief Scientist	Crimson Vista, Inc.
Director of Cybersecurity Research	Curuvar LLC
Adjunct Assistant Professor	University of Texas at Austin Law School
Senior Fellow	Robert Strauss Center for International Security and Law

Professional Advising

2019-Present	Advisory Board	Syccure Inc.
--------------	----------------	--------------

Non-profit and Community Engagement

2021-Present	Founding Director	The Crypto Done Right Foundation
2019-2021	Cyberlab Advisory Board	The SEED School of Maryland

Grants and Research Awards

Decentralizing Zero-Trust Infrastructure to Combat Advanced Persistent Threats and Malicious Insiders (Senior Personnel), NSF 2020 SBIR solicitation. Award number 2051989, Curuvar LLC.

Mitigation of Ransomware, DoD 2018.B STTR solicitation (Army), Topic: A18B-T010, Crimson Vista, \$150,000 (2019)

An Enabling Repository of Cryptographic Knowledge (Co-PI), Cisco Grant, Johns Hopkins University Information Security Institute, \$150,000 (2017-2021)

University Research Funding

Sel4 Security Appliance Capstone, funded by Crimson Vista to Brigham Young University Department of Computer Science. 2021

Academic Awards

Brown Fellowship
John and Eileen Tietze Fellowship

Professional Service

International Cryptographic Module Conference, 2024 Program Committee
International Cryptographic Module Conference, 2023 Program Committee
International Cryptographic Module Conference, 2022 Program Committee
International Cryptographic Module Conference, 2021 Program Committee
International Cryptographic Module Conference, 2020 Program Committee
International Cryptographic Module Conference, 2019 Program Committee
International Cryptographic Module Conference, 2018 Program Committee

Subject Matter Expertise and Selected Projects

Forensic Analysis (e.g., Code/IP Theft)

Investigation of stolen digital documents, provenance, handling (Crimson Vista, 2023-)
Investigation of cryptocurrency transfers and fraud (Crimson Vista, 2023-)
Investigation of website content development and provenance (Crimson Vista, 2023-2024)
Investigation of server, laptop, and hard drives for indications of tampering (Crimson Vista, 2023)
Investigation of voting machine software for vulnerabilities (Crimson Vista, 2022-)
Investigation of altered/forged emails (Crimson Vista, 2022)
CLE training related to source code analysis/trade secrets (Source Code Discovery, 2021)
Investigation of IP/code theft related to MTA, spear-phishing, and email (Crimson Vista, 2019-2021)
Investigation of code theft related to housing and rental software (Crimson Vista, 2019-2022)
Investigation of code development for security vulnerabilities/intrusion (Crimson Vista, 2020)
Investigation of code theft related to digital mobile radios (Crimson Vista, 2017-2021)
Investigation of code theft related to financial trading software (Crimson Vista, 2016-2017)
Investigation of code theft related to e-commerce (Harbor Labs, 2015)
Investigation of IP theft embedded in source code related to domain anti-abuse (Harbor Labs, 2015)
Investigation of IP theft embedded in source code related to high-frequency trading (Harbor Labs, 2010-2011)

Applied Cryptography

Cryptography training modules (UT Austin, 2022-)
Analysis of compromised password hashes (Crimson Vista, 2020)

“Crypto Done Right”, Cryptographic Knowledge Base Non Profit (2020-)

“Crypto Done Right”, Cryptographic Knowledge Base with Cisco (Johns Hopkins, 2017-2020)

Simulated implementation of Vehicle-to-Vehicle authentication (Crimson Vista, 2018-2019)

Cryptographic protocol analysis and design for Syccure Inc. (Crimson Vista, 2017-2023)

Timing attacks on Hardware Security Modules with Diamond Key Security (Johns Hopkins, 2018)

Technical consulting for U.S. Dpt. of Justice (Antitrust Division, Transportation, Energy & Agriculture) (Crimson Vista, 2018)

Aircraft/drone anti-collision protocol security with OnBoard Security (Johns Hopkins, 2017)

Cryptographic communication library for Security First Corp (ISE, 2010-2011)

Encryption library, file system encryption, GPU for Security First Corp (ISE, 2005-2011)

Security Operations, Compliance, Oversight

Security analysis of Twitter cybersecurity operations/practices (Crimson Vista, 2022)

Virtual Chief Information Security Officer for IperionX (Crimson Vista, 2022-2023)

IoT Devices and IoT Security

Traffic lights and systems software analysis (Crimson Vista, 2023-2024)

Vulnerability and exploitation analysis of voting machine hardware (Crimson Vista, 2023-)

High-security appliance based on formal methods (Crimson Vista, BYU, 2021)

Hadoop security research (Crimson Vista, 2021-2022)

IoT data sensors for agricultural operations (Crimson Vista, 2020-2023)

Contributor, reviewer for the Institute of Assured Autonomy (Johns Hopkins, 2019)

IoT data aggregation security with Armored Things (Johns Hopkins, 2018-2019)

Automated IoT device profiling with the Physics Lab (Johns Hopkins, 2018)

Physical forensics from IoT devices (Johns Hopkins 2017)

Network Security

Web security, cookies, XSS, XSRF training modules (UT Austin, 2023-)

Phishing samples analysis (Crimson Vista, 2022-2023)

WiFi transmission analysis, packet capture (Crimson Vista, 2023-)

Security-Focused Data Discovery Methods and Practice (Crimson Vista, 2022-2023)

Analysis of weaknesses in two-factor authentication (Crimson Vista, 2022-2023)

Analysis of bots on Twitter in terms of prevalence, stealth, and impact (Crimson Vista, 2022)

Secure distributed computing (Curuvar, 2021-2023)

Hadoop deployment and security considerations (Crimson Vista, 2021-2022)

SSO technology evaluation and test (UT Austin, Crimson Vista, 2021-2022)

Information risk assessment with respect to data breach (Crimson Vista, 2020-2021)

Data breach analysis with respect to password authentication (Crimson Vista, 2020-2021)

Network security curriculum design for Law and Policy (University of Texas at Austin, 2020-)

Network security curriculum design for undergraduates (University of Texas at Austin, 2020-2021)

Network security curriculum design (Johns Hopkins, 2013-2019)

Security analysis of financial services vendor for Fortune-100 client (Crimson Vista, 2018-2019)

Analysis of secure e-mail transmission for confidential client (Crimson Vista, 2018-2019)

Cloud storage system security evaluation for confidential client (Harbor Labs, 2015)

Secure gateway security and compliance evaluation for SecurityFirst Corp (Harbor Labs, 2015)

Gateway caching security/privacy engineering (Google, 2005)

Malware and Viruses

Ransomware training modules (UT Austin, 2022-)

Ransomware recovery research and development (Crimson Vista, 2018-2019)

Advanced malware and malware defenses analysis (Johns Hopkins, 2018)

Malware Analysis for Confidential Client (Crimson Vista, 2016)

Privacy

Investigation of location tracking in mobile devices (Crimson Vista, 2021-)

Investigation of biometric tracking/transmission in devices and systems (Crimson Vista, 2021-)

Development of an auditing tool for cookies and other web tracking (Crimson Vista, 2020)

Audit of a large hospital network for cookies and web tracking (Confidential client, 2020)

Development of a privacy curriculum for data architects (Crimson Vista, 2019)

Anonymization of threat indicators with the Applied Physics Lab (Johns Hopkins, 2017)

Analysis of anti-piracy vendor for Center for Copyright Information (Harbor Labs, 2013-2014)

Miscellaneous Security Technologies

Distributed ledger technology for secure state replication (Curuvar, 2021-2023)

Blockchain technology for sale and/or licensing of intellectual property (Crimson Vista, 2021-2022)

Blockchain technology analysis for a start-up (Crimson Vista, 2019-2020)

Analysis of cyber security norms for a confidential Fortune 100 client (Crimson Vista, 2018-2019)

Analysis of vulnerabilities in portable chemical manufacturing system (Johns Hopkins, 2018)

Open-Source Contribution and Sponsorship for The PyPy Project (Crimson Vista, 2018-2019)

Blockchain and smart contract design for confidential start-up (Crimson Vista, 2018)

Medical device system security evaluation for confidential client (Harbor Labs, 2015)

Software Engineering and Software Analysis

Review of development practices, error handling, and robustness (Crimson Vista, 2023-)

Open-source licensing analysis, build, and test (Crimson Vista, 2023-)

GitHub analysis and statistics for effort estimation (Crimson Vista, 2022)

Software theft analysis and tool design for various clients (Crimson Vista, 2018-)

Cyber insurance investigations for Clyde & Co (Crimson Vista, 2018-2019)

Distributed code coverage analysis tool for a confidential Fortune 100 client (ISE, 2011)

Software engineering for Metrowerks Inc. (2001-2003, formerly Lineo Inc.)

Code Languages: C, C++, Java, Python, Ruby, Scala, RTL/VHDL/Verilog, JavaScript, Go

Publications

Books

Seth James Nielson, *Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner*. (December 2023).

Seth James Nielson, Christopher K. Monson, *Practical Cryptography in Python, Learning Correct Cryptography by Example*. (October 2019).

Refereed Publications

Joseph Kosturko, Eric Schlieber, Sean Futch, Seth James Nielson, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices*. In *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security*. (September 2018)

Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson, Timothy Leschke, *Potential Forensic Analysis of IoT Data: An Overview of Amazon Echo, Z-wave, and Home Router Data Extraction and Analysis*. In *Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings)*, Exeter, UK, pp. 705-710 (June 2017).

Seth James Nielson, *PLAYGROUND: Preparing Students for the Cyber Battleground*. *Computer Science Education*, volume 26, issue 4, pp. 255-276, (January 2017).

Seth James Nielson and Charles D. Knutson, *Design Dysphasia and the Design Patterns Maintenance Cycle*. *Information & Software Technology*, volume 48, number 8, pp. 660- 675, (August 2006)

Seth James Nielson, Scott S. Crosby, and Dan S. Wallach, *A Taxonomy of Rational Attacks*. In *Proceedings of the Fourth International Workshop on Peer-to-Peer Systems (IPTPS '05)*, Ithaca, New York, (February 2005)

Seth J. Nielson and Charles D. Knutson. *OO++: Exploring the Multiparadigm Shift*. *Proceedings of the Workshop on Multiparadigm Programming with Object-Oriented Languages (MPOOL 2004)*, Oslo, Norway, (June 2004)

Rob Kunz, Seth Nielson, Mark Clement, Quinn Snell, *Effective Bandwidth for Traffic Engineering*, *Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR 2001)*, Dallas, TX, (May 2001)

Testimony Before Government Bodies

Testimony in support of *Maryland SB 151/HB 211 Criminal Law - Crimes Involving Computers – Ransomware*. Testimony given to the Judicial Proceedings Committee of the Maryland Senate and the Judiciary Committee of the Maryland House of Delegates (January/February 2019)

Invited Talks, Panels, and Technical Training

Seth James Nielson, *Data Security: Four Approaches to a Better Defensive Posture*, 2023 Enterprise Data World, Anaheim, CA (September 2023)

[CANCELED DUE TO VENUE CHANGE] Seth James Nielson, *Maintaining Data Security and Data Privacy in the 21st Century*, 2022 Enterprise Data World, San Diego, CA (March 2022)

Seth James Nielson, *Securing Your Data Assets Against Hackers*, 2021 Enterprise Data World, Boston, MA. (April 2021)

Seth James Nielson, *The Cybersecurity of IP*, 2020 Essential Cybersecurity Law, Austin, TX (Virtual). (July 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson and Ellie Daw, *Correct Cryptography in Python*, a Tutorial for Cryptography Beginners, PyCon 2020, Philadelphia, PA. (April 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson, *Protecting Your Data Assets*, 2020

Enterprise Data World, Boston, MA. (March 2020)

Seth James Nielson, *Security and Privacy for Data Architects*, 2019 Data Architecture Summit, Chicago, IL (October 2019)

Seth James Nielson, *Crypto Done Right, One Year In. Lessons Learned and Next Steps*. Presented in the International Cryptographic Knowledge Base 2019 (ICMC 2019), Vancouver, Canada (May 2019)

Panel Discussion, *Hardening US Unmanned Systems Against Enemy Counter Measures*. Accepted invitation to 7th Annual DoD Unmanned Systems Summit, Alexandria, VA (April 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2019 Enterprise Data World, Boston, MA (March 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2018 Data Architecture Summit, Chicago, IL (October 2018).

Seth James Nielson, *Detecting Malicious Sandboxes*. Workshop on Defensive Deception and Trust in Autonomy, San Diego, CA (August 2018).

Seth James Nielson and Debra Baker, *Towards a Crowd-Sourced Cryptographic Knowledge Base*. Presented in the International Cryptographic Knowledge Base 2018 (ICMC18), Ottawa, Canada (May 2018).

Seth James Nielson, *The PyPy Sandbox*. Presented in the National Centers of Academic Excellence Tech Talk, Online (March 2018).

Theses

PhD Thesis: Designing Incentives for Peer-to-Peer Systems (defended 10/2009)

Master's Thesis: OO++ Design Patterns, GOF Revisited (defended 8/2004)

Technical Reports

Seth James Nielson and Dan S. Wallach, *The BitTorrent Anonymity Marketplace*, arXiv Technical Report 1108.2718, (August 2011)

Seth James Nielson, Caleb E. Spare, and Dan S. Wallach, *Building Better Incentives for Robustness in BitTorrent*, arXiv Technical Report 1108.2716, (August 2011)

Seth James Nielson, Seth J. Fogarty, and Dan S. Wallach, *Attacks on Local Searching Tools*, arXiv Technical Report 1108.2704 (Originally produced in December, 2004, available on arXiv as of August 2011)

White Papers and Trade Publications

Seth James Nielson, *Techniques for Discovering Unauthorized Copying in Software*, Crimson Vista White Paper, (January 2022)

Aviel D. Rubin, Seth J. Nielson, Christopher K. Monson, *Evaluation of the MarkMonitor AntiPiracy System*, Produced for the Center for Copyright Information (December 2013)

Aviel D. Rubin, Seth J. Nielson, Sam Small, Christopher K. Monson, *Guidelines for Source Code Review in Hi-Tech Litigation*, Harbor Labs White Paper (September 2013)

Undergraduate Advising

Independent Research and Capstones (University of Texas Austin)

Triambika Dinakaran, *Identification of Bots in Online Reviews* [Tentative Project], CS 370, Independent Study, Expected Summer 2024

Andrew Dang, *Individual Voice Recognition using Machine Learning*, CS 370, Independent Study, Summer 2023

Monique Tran, *Malware Classification with SVM*, CS 370, Independent Study, Summer 2023

Gonzalo Tamariz-Martel Sánchez, *SMART CONTRACTS: Different approaches to introduce external (off-chain) data* (June 2022)

Graduate Advising

Capstones for Masters of Science in Security Informatics (Johns Hopkins)

Weizhou Wang, Runjie Zhang, *Research on defense next-generation malware on the Windows platform* (December 2018)

Yu-Tsern Jou, Ying Liu, Menghan Bai, *Open Source HSM Side Channel Analysis* (December 2018)

Bowen Shi, Hong Ma, Mengqi Qin, *Side Channel Attack on HSM Based on Machine Learning* (December 2018)

Dylan Richmond, Matthew Shonman, Jingcheng Yang, *An Exploration of the Usability of HTTPS* (December 2018)

Steven Cheng, Venkata Aditya Bollapragada, and Antara Sargam, *Using Selective RAM Journaling to Fight Ransomware* (December 2018)

Yongqiang Fan, Haiwen Sun, *Fault Tolerance System for IoT* (December 2018)

Wei-ke Chen, Harry Luo, Prashanth Venkateswaran, *IoT Discovery* (August 2018)

Joseph "Jay" Kosturko, Eric Schlieber, Sean Futch, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices* (May 2018)

Chao Lei, Wenjun Li, *Anti-Honeypot Detection in Advanced Botnet Attacks* (December 2017)

Ritvik Sachdev, Purushottam Kulkarni, Praveen Malhan, *Securing ADS-B Based Airborne Collision Avoidance Systems* (December 2017)

Ningyuan Bao, Mengying Hu, *Security-Testing-Orientated Internet of Things(IoT) Simulator* (December 2017)

Zehuan Li, Shanshan Yang, Liangjia Fu, *AIS Data De-anonymization* (December 2017)

Chanyang Shin, Prerit Chandok, Aurin Chakravarty, *Forensic Data Collection from IoT Devices* (December 2017)

Kevin Manzotti, Kashif Memon, Rahul Durgad, *Replication of CryptoDrop* (December 2016)

Harshneel More, Jingmiao Wang, Yuanqi Zhu, *Detecting XSS attacks using BRO IDS* (December 2016)

Asmaa Aljohani, Gyan Namdhari, Yue Zhu, *Feasibility, Security and Privacy Analysis of EMVCo Payment Tokenization Technology for Identity Enabled Transactions* (December 2016)

Richard Eaton, *The Emperor Has No Friends: Identifying Botnet Customers and Mapping Out Botnets on Twitter* (May 2015)

Jingru Chen, Yaning Liu, Yifan Yu, Zhiyue Zu, *Investigating the Heartbleed Vulnerability* (2015)

Kartik Thapar, *Security Techniques for Developing iOS Applications* (February 2015)

Jie Feng, Jianxiang Peng, Likai Zhang, *De-anonymizing BitCoin* (January 2014)

Teaching

University of Texas at Austin

Cybersecurity Tech/Law Policy (2020-)
Network Security and Privacy (2020-2021)

Johns Hopkins University

Advanced Network Security (2017 - 2019)
Network Security (2014 – 2019)

Rice University

Data Structures and Algorithms (Spring 2008)

Patents

Co-inventor: Nielson, S. 2021. Distributed Authentication Between Network Nodes. U.S. Patent 11,032,252 filed January 2, 2019 and issued June 8, 2021.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,372 filed November 24, 2010 and issued June 3, 2014.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,379 filed August 20, 2012 and issued June 3, 2014.

Co-inventor: O'Hare, R. 2014. Systems and methods for security data. U.S. Patent 8,677,148 filed January 27, 2012 and issued March 18, 2014.

In the News

"Johns Hopkins Researchers and OnBoard Security Team Up to Protect Drones," *Robotics Tomorrow*, 3/16/2018

"Rice University Computer Scientists Find a Flaw in Google's New Desktop Search Program." *New York Times*, 12/20/2004

Employment History

University of Texas at Austin

2020-

Adjunct Assistant Professor

Source Code Discovery, LLC.

2019-2021

Founder and Partner

Crimson Vista, Inc.

2016-Present

Founder and Chief Scientist

Johns Hopkins Applied Physics Lab

2018-2019

Senior Professional Staff (Temp/On-Call)

Johns Hopkins University

2016-2019

Director of Advanced Research Projects

2015-2019

Adjunct Associate Research Scientist

2014

Lecturer

Harbor Labs, LLC

2014-2015

Principal

2011-2014

Research Scientist

Independent Security Evaluators

2010-2011

Senior Security Analyst

2005-2009

Security Analyst

Google, Inc.

2005

Summer Intern

Metrowerks (Formerly Lineo, Inc.)

2001-2003

Software Engineer II

Expert Testimony

On behalf of Forescout Technologies in Fortinet v Forescout Technologies

Counsel: Winston & Strawn

Venue: Northern District of California

Subject Matter: Network security architecture and devices

Reports: 1 report March 2024

On behalf of Threat Modeler Software in Iriusrisk v Threat Modeler Software

Counsel: Rimon
Venue: PTAB
Subject Matter: Threat modeling
Reports: 1 declaration January 2024, 1 declaration February 2024
Deposition: March 2024

On behalf of Motorola Solutions in Motorola Solutions v. Hytera Communications

Counsel: Kirkland and Ellis
Venue: Northern District of Illinois, Eastern Division
Subject Matter: Source code forensics
Reports: 1 declaration January 2024
Deposition: February 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 7,586,871

Counsel: Univied Patents
Venue: PTAB
Subject Matter: Network security and data filtering
Reports: 1 declaration, February 2024

On behalf of the State of Texas in State of Texas v. Google

Counsel: Norton Rose Fulbright
Venue: District Court of Victoria County Texas
Subject Matter: Location tracking
Reports: 1 report, January 2024

In support of Unified's Request for Ex Parte Reexamination of U.S. Patent 9,264,441

Counsel: Rothwell, Figg, Ernst, and Manbeck
Venue: PTAB
Subject Matter: Network security devices and operations
Reports: 1 declaration, January 2024

On behalf of Dennis Zeedyk in the United States vs. Dennis Zeedyk (2023-Present)

Counsel: Saul Euwing
Venue: Northern District of Indiana South Bend Division
Subject Matter: Website forensics
Reports: 1 report November 2023

On behalf of OpenAI in OpenAI v Open Artificial Intelligence and Guy Ravine (2023-Present)

Counsel: Quinn Emanuel
Venue: Northern District of California
Subject Matter: Forensic investigation of website and related assets
Reports: 1 report October 2023

On behalf of Palo Alto Networks in Centripetal Networks v Palo Alto Networks (2021-Present)

Counsel: Norton Rose Fulbright and Ropes & Gray
Venue: Eastern District of Virginia
Subject Matter: Network security devices
Reports: 3 reports issued August 2023, September 2023, and October 2023

Deposition: October 2023
In Court: January 2024

On behalf of Anchor Semiconductor in Elite v. Anchor (2022-Present)

Counsel: Venable
Venue: Northern District of California
Subject Matter: Forensic investigation of alleged sabotage and data destruction
Reports: 1 report July 2023

In support of Unified Patents in Ex Parte Reexamination of U.S. Patent 9,438,614

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Machine learning and intrusion detection systems
Reports: 1 declaration Apr 2023

On behalf of Trend Micro in Trend Micro v. TaaSera Licensing (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 4 declarations Apr 2023

On behalf of Salesforce in WSOU Investments v. Salesforce (2022-Present)

Counsel: Quinn Emanuel
Venue: Western District of Texas
Subject Matter: Source code related to transmission of marketing emails
Reports: March 2023
Deposition: August 2023

On behalf of Trend Micro in Trend Micro v. Webroot (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 5 declarations Feb-Mar 2023, 5 declarations September 2023

On behalf of Fox News in Dominion Voting Systems v. Fox News (2022-2023)

Counsel: Winston and Strawn
Venue: Superior Court of the State of Delaware
Subject Matter: Voting machine security including forensic investigation
Reports: 1 Report December 2022
Deposition: February 2023

On behalf of Public Storage in Estch v. Public Storage (2022-2023)

Counsel: Orrick
Venue: Eastern District of Texas
Subject Matter: VoIP, authentication, authorization
Reports: 1 Report January 2023
Deposition: January 2023

On behalf of Lenovo/Motorola Mobility in Maxell Ltd v. Lenovo/Motorola Mobility (2022-2023)

Counsel: Kirkland and Ellis
Venue: ITC
Subject Matter: Authentication
Reports: 1 Declaration November 2022
2 Reports February 2023
Deposition: March 2023

On behalf of Elon R Musk in Twitter Inc v. Elon R Musk (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Court of Chancery of the State of Delaware
Subject Matter: Evaluation of Security in light of Whistleblower Report
Reports: 1 Report October 2022

On behalf of Bissell, Inc. in Bissell Inc. v. Tineco Intelligent Technology Co. Ltd., (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: ITC
Subject Matter: Forensic evaluation of source code
Reports: 1 Report submitted September 2022
Deposition: November 2022
In Court: December 2022

On behalf of Hakkasan USA in Hakkasan USA v Endurance American Specialty Insurance (2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: District of Nevada (Clark County)
Subject Matter: Forensic evaluation of emails
Reports: 1 Report submitted May 2022
Deposition: July 2022

On behalf of JTC in Seimens vs JTC (2021-2022)

Counsel: Peckar and Abramson, PC
Venue: American Arbitration Association
Subject Matter: Software Engineering Efforts
Reports: 1 Report submitted in July 2021
1 Report submitted in September 2021
Deposition: October 2021
In Court: March 2022 (arbitration)

On behalf of Samsung in Samsung v. Proxense (2021-2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Western District of Texas (Waco)
Subject Matter: Authentication, Authorization, Device-to-device
Reports: 1 declaration submitted October 2021
Deposition: October 2022

On behalf of Bitglass in Netskope, Inc. v. Bitglass Inc. (2021-2022)

Counsel: Irell and Manela, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Authentication, Single-Sign-On
Reports: 1 declaration submitted September 2021

1 declaration submitted March 2021

On behalf of The State of Arizona in Arizona v. Google (2021-2022)

Counsel: Ruttenberg IP Law
Venue: Superior Court of the State of Arizona (Maricopa)
Subject Matter: Privacy, Location tracking, Data collection
Reports: 1 declaration submitted August 2021

On behalf of TLC in TLC v. Koninklijke Philips N.V., US Philips Corporation (2019-2021)

Counsel: Perkins Coie LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Cryptographic protocols
Reports: 1 declaration submitted February 2021

On behalf of Magic Micro in Monsoon v. Magic Micro (2020-2021)

Counsel: Gutnicki, LLP
Venue: International Centre for Dispute Resolution
Subject Matter: Blockchain, file storage
Reports: 1 declaration submitted October 2020
1 declaration submitted November 2020
In Court: In arbitration December 2020

On behalf of Juniper in Juniper Networks Inc. v. Huawei Digital Technologies Co. (2020-2021)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Network perimeter defense against malware
Reports: 1 declaration submitted June 2020
1 declaration submitted July 2021
Deposition: April 2021

On behalf of DivX in Netflix v. DivX (2020-2023)

Counsel: Lowenstein & Weatherwax, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Encryption of streaming media
Reports: 1 declaration submitted May 2020
1 declaration submitted December 2020
1 declaration submitted April 2021
Deposition: January 2021, February 2021

On behalf of Juniper in Juniper Networks Inc. v. Implicit LLC (2019-2020)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Packet classification
Reports: 1 declaration submitted February 2020

On behalf of the Dealership class in Dealer Management Systems Antitrust Litigation (2019-Present)

Counsel: Milberg Phillips Grossman LLP
Venue: Case No. 18-cv-00864 (Northern District of Illinois)

Subject Matter: Cybersecurity, risk assessment, third-party access
Reports: 1 report submitted November 2019
Deposition: January 2020

On behalf of Symantec in the Trustees of Columbia University in the City of New York v. Symantec Corporation. (2018-2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. Civil Action No. 3:13-cv-00808-JRS (Eastern District of Virginia)
Subject Matter: Deception technologies, Honeypots
Reports: 1 report submitted October 2019
Deposition: January 2020

On behalf of Proofpoint in Proofpoint Inc. v. Vade Secure (2019-2021)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. 3:19-cv-04238 (Northern District of California)
Subject Matter: Cloud-based email, malware detection, AI
Reports: 1 report submitted September 2019, 1 report submitted December 2019
1 report submitted February 2021, 1 report submitted April 2021
Deposition: April 2021
In Court: Expert testimony August 2021

On behalf of Bitdefender in Finjan Inc. v. BitDefender Inc. (2018-2021)

Counsel: Susman Godfrey LLP
Venue: Case No. 4:17-cv-4790-HSG (Northern District of California)
Subject Matter: Web threat detection, malware, gateways
Reports: 1 report submitted July 2019, 1 report submitted August 2019
Depositions: October 2019

On behalf of HTC in Koninklijke Philips N.V., US Philips Corporation v. HTC Corp., HTC America Inc. (2019-2020)

Counsel: Perkins Coie LLP
Venue: Case No. 4:18-cv-01887-HSG (Northern District of California)
Subject Matter: Cryptographic protocols
Reports: 1 report submitted May 2019, 1 report submitted June 2019
Depositions: August 2019

On behalf of Juniper in Juniper Networks Inc. v. Finjan Inc. (2018-2019)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Malware, firewall/gateway, network security
Reports: 4 declarations submitted October 2018
Depositions: June 2019

On behalf of Redbox in Disney Enterprises, Inc., LucasFilm Ltd, LLC, and MVL Film Finance LLC v. Redbox Automated Retail, LLC. (2018)

Counsel: Robins Kaplan LLP
Venue: Case No. 2:17-cv-08655-DDP (AGRx) (Central District of California, Western Division)
Subject Matter: DRM, cloud security, media streaming

Reports: 1 declaration submitted May 2018

On behalf of Trend Micro in Trend Micro, Inc. v. Security Profiling, LLC (2017-2018)

Counsel: The Marbury Law Group, PLLC

Venue: Inter Partes Review Case No. IPR2017-02191 and IPR2017-02192

Subject Matter: Automated security patches

Reports: 2 declarations submitted September 2017

Depositions: June 2018

On behalf of TeleSign in Twilio Inc. v. TeleSign Corporation (2016-2021, multiple cases)

Counsel: Shook, Hardy & Bacon LLP

Venue: Inter Partes Review Case No. IPR2016-01688, IPR2016-00360, IPR2017-01976 IPR2017-01977, IPR2017-01978
Case No. 5:16-cv-6925-LHK (Nor. District of California, San Jose Div.)

Subject Matter: Telecommunications security

Reports: 1 declaration submitted August 2016, May 2017, and July 2017

Depositions: November 2016, July 2017, August 2017

On behalf of Blue Coat in Finjan Inc. v. Blue Coat Systems LLC (2017-2018)

Counsel: Originally Wilson, Sonsini, Goodrich and Rosati PC; later Morrison & Foerster LLP

Venue: Case No. 15-cv-03295-BLF-SVK (Nor. District of California, San Div.)

Subject Matter: Firewalls, gateway, security devices, malware

Reports: 1 report submitted April 2017

Depositions: April 2017

In Court: Tech tutorial February 2017, expert testimony November 2017

On behalf of Sedosoft in Sedosoft Inc. v Mark Burchett LTD and NFSx9 LLC (2016)

Counsel: McInnes and McLane LLP

Venue: Case No. Civil Action No. 1:15-cv-10244-RGS (District of Massachusetts)

Subject Matter: Code theft

Reports: 1 report submitted May 2016 and August 2016

On behalf of USAA in Asghari-Kamrani, et al. v. United Services Automobile Association, Inc.

Counsel: Fish and Richardson PC

Venue: Inter Partes Review Case No. IPR2015-01842, and CBM2016-00063, CBM2016-00064

Subject Matter: Applied cryptography, authentication

Reports: 1 report submitted September 2015, 1 report submitted April 2016

Depositions: March 2017

On behalf of WTS Paradigm in WTS PARADIGM, LLC v EDGEAQ, LLC (2015-2016)

Counsel: Quarles & Brady LLP

Venue: Case No. 3:15-CV-330 (Western District of Wisconsin)

Subject Matter: Software-assisted product configuration, presentation, and ordering

Reports: 1 report submitted March 2016

Depositions: April 2016

On behalf of Mr Leon Stambler in Mr. Leon Stambler v Mastercard IPR (2015-2016)

Counsel: Flachsbart & Greenspoon, LLC
Venue: CBM2015-00044
Subject Matter: Authentication, authentication codes
Reports: 1 declaration submitted October 2015
Deposition: December 2015

On behalf of Trusteer/IBM in Trusted Knight Corporation v. International Business Machines Corporation and Trusteer, Inc. (2015)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: C.A. No. 14-1063 LPS-CJB (District of Delaware)
Subject Matter: Key logging, protections against
Reports: 1 declaration submitted July 2015

On behalf of Sensus in Sensus USA, Inc. v. Certified Measurement, LLC (2015)

Counsel: Feldman Gale PA
Venue: Inter Partes Review Case No. IPR2015-01262, IPR2015-01311, IPR2015-01439, IPR2015-01454
Case number 3:14-cv-01069 (District of Connecticut)
Subject Matter: Applied cryptography, certification of data
Reports: 1 declaration submitted June 2015, 4 declarations submitted July 2015

On behalf of Chad Eichenberger in Chad Eichenberger v. ESPN (2015)

Counsel: Edelson PC
Venue: Case No. 2:14-cv-00463 (Western District of Washington)
Subject Matter: Consumer privacy
Reports: 1 declaration submitted January 2015

On behalf of Optimum Content Protection in Microsoft Corporation v. Optimum Content Protection LLC. (2014)

Counsel: Sidley Austin LLP
Venue: Inter Partes Review No. IPR2015-00048
Subject Matter: DRM, data streaming, protection
Reports: 1 declaration submitted October 2014

On behalf of Fortinet in Fortinet v. Sophos (2014-2015, multiple cases)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: Inter Partes Review No. IPR2015-00618
Case No. 3:13-cv-05831-EMC (DMR) (Nor. District of California, SF div.)
Case No. 1:14-cv-00100-GMS (District of Delaware)
Subject Matter: Antivirus, anti-malware
Reports: 2 declarations submitted September 2014, 1 submitted September 2015
1 report submitted October 2015, November 2015
Depositions: October 2014, October 2015
In Court: Tech tutorial December 2015

On behalf of Afiliis in Afiliis PLC v Architelos Inc and Alexa Raad (2015)

Counsel: Haynes Boone LLP
Venue: Case No. 1:15-cv-00014-LMB-JFA (Eastern District of Virginia)
Subject Matter: Domain name system anti-abuse

Reports: 1 report submitted April 2015, May 2015
Depositions: June 2015
In Court: Expert testimony August 2015

On behalf of Telit in M2M v. Motorola, Telit (2015-2016)

Counsel: Pearl Cohen Zedek Latzer Baratz LLP
Venue: Case No. 12-033-RGA (District of Delaware)
Subject Matter: Authentication
Reports: 1 declaration submitted May 2014,
1 report submitted July 2014, August 2014
Depositions: June 2015

On behalf of Rmail/Rpost in Rmail Limited, v. Amazon.com, Inc., and Paypal and Rmail Limited, Rpost Communications Limited, and Rpost Holdings Inc., v. Docusign, Inc. (2013-2014)

Counsel: Hudnell Law Group PC
Venue: Case No. 2:10-CV-258-JRG (Lead Case)
Case No. 2:11-CV-299-JRG (Member Case) (E.D. Texas)
Subject Matter: Email security
Reports: 2 reports April 2013, 1 declaration June 2013
Depositions: May 2013 (2 days)

On behalf of Via Vadis in Via Vadis v. Skype (2012-2014)

Counsel: WTP Law
Venue: Via Vadis v. Skype, Case No. 11-507 (RGA) (District of Delaware)
Subject Matter: P2P communications
Reports: 1 affidavit December 2012