UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

CISCO SYSTEMS, INC.,
Petitioner,

v.

CENTRIPETAL NETWORKS, INC.,
Patent Owner.

_____

Case No. IPR2018-01512
Patent No. 9,565,213

DECLARATION OF DR. MICHAEL GOODRICH IN SUPPORT OF PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

Page

I, Michael T. Goodrich, Ph.D., make this declaration based upon my own personal knowledge, information, and belief:

I. EXPERIENCE AND QUALIFICATIONS

A. Curriculum Vitae

1. My experience and education are detailed in my curriculum vita, which is attached as Appendix A to this report.

2. I received a Bachelor of Arts ("BA") degree in Mathematics and Computer Science from Calvin College in 1983 and a Ph.D. in Computer Sciences from Purdue University in 1987.

3. I am a Distinguished Professor in the Department of Computer Science at the University of California, Irvine, where I have been a faculty member since 2001. The Distinguished Professor title is a campus-level distinction and is reserved for faculty who have achieved the highest levels of scholarship over the course of their careers. In addition, I am the technical director for the Center for Algorithms and Theory of Computation in the Donald Bren School of Information and Computer Sciences at University of California, Irvine. I was a professor in the Department of Computer Science at Johns Hopkins University from 1987-2001.

4. I have authored or coauthored over 300 publications, including several widely adopted books, such as *Introduction to Computer Security* and *Algorithm Design and Applications*. My research includes contributions to data structures and

algorithms, information security and privacy, networking, graph algorithms, computational geometry, distributed and parallel algorithms, and cloud security. For example, I have published research articles about tracing network attacks, authenticating users and data to prevent intrusions and viruses, and certifying email messages to stop malware attachments. My research has been supported by grants from the Defense Advanced Research Projects Agency (DARPA) from the National Science Foundation (NSF).

5. I have served on proposal review panels for the NSF and have served as a program chair or member of the program chair or member of the technical program committee for many peer-reviewed conferences, workshops, and symposia in Computer Science, including ACM Symposium on Theory of Computing (STOC), IEEE Symposium on Foundations of Computer Science (FOCS), ACM-SIAM Symposium on Discrete Algorithms (SODA), ACM Conference on Computer and Communication Security (CCS), IEEE Symposium on Security and Privacy (S&P), IEEE International Conference on Data Engineering (ICDE), IEEE International Parallel & Distributed Processing Symposium (IPDPS), International Conference on Applied Cryptography and Network Security (ACNS), International Colloquium on Automata, Languages and Programming (ICALP), European Symposium on Algorithms (ESA), ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), International

Symposium on Graph Drawing (GD), Symposium on Computational Geometry (SoCG), and Workshop on Algorithm Engineering and Experimentation (ALENEX), the latter of which I also co-founded.

6. I am a named inventor on four U.S. Patents. These patents are generally related to networking and the delivery of services over the networks, as well as computer and information security and computer animation.

7. In addition, I have experience consulting and testifying as an expert in matters involving algorithms, cryptography, machine learning, digital rights management, computer security, networking, software, and storage technologies. A list of cases in which I have testified at deposition or trial or have provided written declarations and reports, including *inter partes* reviews, during at least the past five years is part of Appendix A of this Report.

8. I am an ACM Distinguished Scientist, a Fellow of the American Association for the Advancement of Science (AAAS), a Fulbright Scholar, a Fellow of the institute of Electrical and Electronics Engineers (IEEE), and a Fellow of the Association for Computing Machinery (ACM). I am also a recipient of the IEEE Computer Society Technical Achievement Award and the Pond Award for Excellence in Undergraduate Teaching. In addition, I have been named as a foreign member of the Royal Danish Academy of Sciences and Letters.

B. Compensation

9. My rate of compensation for my work in this case is $650 per hour plus any direct expenses incurred. My rate of compensation is based solely on the amount of time that I devote to activity related to this case and is in no way affected by any opinions that I render. I receive no other compensation from work on this action. My compensation is not dependent on the outcome of this matter.

II. SCOPE OF STUDY AND OPINIONS

A. Materials Considered

10. My opinions, expressed herein, are based on information I have reviewed to date including but not limited to the materials referenced herein and in the exhibits attached to this report, and are based on my knowledge and experience in the fields of computer and network security optimization.

11. I expect to review any reports and/or declarations submitted by the retained expert of the opposing party in this matter and I expressly reserve the right to amend or supplement this declaration, as appropriate, after considering the opinions set forth in any reports or declarations submitted by the retained expert of the opposing party or any additional information produced by the Petitioner after the date of this declaration.

12. In the process of forming my opinions, I have reviewed and considered numerous documents and items including, but not limited to: the expert

declaration of Dr. Jeffay, including all documents cited in his declaration, including the Centripetal Patents and their file histories, the PTAB's institution decision for this case, and various cited documents, including alleged prior art.

B. Summary of Opinions

13. I have been asked by counsel for Centripetal to consider the following grounds of invalidity in the Petition and Dr. Jeffay's declaration:

- Claims 1–9 are rendered obvious by ACNS in view of Kjendal.
- Claims 10–16 are rendered obvious by ACNS in view of Kjendal and the DiffServ Specification.

14. It is my opinion that Cisco's position and Dr. Jeffay's final conclusion regarding the above grounds of invalidity are incorrect. It is my opinion that all of the instituted claims of the '213 Patent are valid. Furthermore, it is my opinion that Cisco failed to provide sufficient evidence to prove that the instituted claims of the '213 Patent are invalid.

III. LEGAL STANDARDS

15. Counsel for Centripetal has informed me of the following legal standards that I have used as a framework in forming my opinions contained herein:

A. Anticipation

16. I have been informed that a patent claim is anticipated if each and every limitation of that claim is disclosed either explicitly or inherently in a single prior art reference. If not explicitly disclosed, a limitation is inherently disclosed in a prior art reference if an unstated limitation is necessarily included in the prior art.

17. I have been informed that, in order for a prior art reference to anticipate a patent claim, the reference must also enable one of ordinary skill in the art to make or practice the claimed invention without undue experimentation.

18. I have been informed that under pre-AIA law, if an invention reflected in a patent claim was known or used by others in the United States, or patented or described in a printed publication in the United States or a foreign country, before the invention date of that patent claim, then the patent claim at issue is invalid under 35 U.S.C. § 102(a).

19. I have been informed that if an invention reflected in a patent claim was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country more than one year before the earliest priority date for that patent claim, then the patent claim is invalid under 35 U.S.C. § 102(b).

20. I have been informed that if an invention reflected in a patent claim was disclosed in another patent that was granted from a United States patent application filed before the invention date of the patent claim at issue, then the patent claim at issue is invalid under 35 U.S.C. § 102(e).

21. I have been informed that if an invention reflected in a patent claim was invented before the invention date of the patent claim at issue by another inventor in the United States and not abandoned, suppressed, or concealed by that earlier inventor, then the patent claim is invalid under 35 U.S.C. §102(g).

22. I have been informed that under post-AIA law, a patent claim is anticipated if each and every limitation of that claim is disclosed either explicitly or inherently in a single prior art reference that predates the effective filing date of the patent claim unless the prior art reference is owned by the same entity or has overlaps of inventorship, in which case, the reference is not considered as prior art unless it is dated more than one year of the effective filing date of the patent claim.

B. Obviousness

23. I have been informed that even if a single reference does not contain every limitation of a patent claim, it can still invalidate that claim if it renders the claimed invention obvious when considered in light of other prior art references or devices. If the differences between the claimed invention and the prior art are such that the claimed invention, as a whole, would have been obvious to a person

having ordinary skill in the art at the time the invention was made without the benefit of hindsight, then the claim is invalid.

24. I have been informed that the types of 35 U.S.C. §102 prior art described above can individually be a basis for invalidating a patent, or these references can be combined to show a patent is invalid as obvious under 35 U.S.C. §103.

25. I have been informed that the analysis of obviousness involves several factual inquiries including the scope and content of the prior art, the differences between the prior art and the claim, and the level of ordinary skill in the art at the time of the invention.

26. I have been informed that a reference qualifies as prior art for obviousness purposes when it is analogous to the claimed invention. The test for determining what art is analogous is: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.

27. I have been informed that to determine whether a combination of known elements would have been obvious to a person of ordinary skill in the art at the time of the invention, one must consider the references in their entirety to

ascertain whether the disclosures in those references render the combination obvious to such a person.

28. I have been informed that the combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. Additionally, I understand that a patent is likely to be invalid for obviousness if a person of ordinary skill in the art can implement a predictable variation or if there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. A combination is not obvious, however, where the combination cannot be implemented without undue experimentation or when the motivation to create the combination comes from hindsight.

29. I have been informed that when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill in the art has good reason to pursue the known options within his or her technical grasp. I understand that, if this leads to anticipated success, it is likely the product not of innovation, but rather of ordinary skill and common sense. I have been informed that the fact that a combination was obvious to try might show that the patent claim was obvious.

30. I have been informed that, even when all claim limitations can be found in a combination of prior art references, the fact-finder must consider as part

of the obviousness determination not only what the prior art teaches, but whether the prior art teaches away from the claimed invention and whether there is a motivation to combine teachings from separate references in the manner claimed.

C. Objective Indicia of Nonobviousness

31. I have been informed that relevant considerations in a determination of invalidity based on obviousness must include consideration of objective indicia of non-obvious, otherwise known as secondary considerations of non-obviousness. I understand that objective indicia of both non-obviousness should be considered when evaluating whether a claimed invention would have been obvious to one of ordinary skill in the art at the time of invention. These secondary indicia may include, for example:

a. a long felt but unmet need in the prior art that was satisfied by the claimed invention;

b. commercial success of processes claimed by the patent;

c. unexpected results achieved by the invention;

d. praise of the invention by others skilled in the art;

e. the taking of licenses under the patent by others; and

f. deliberate copying of the invention.

IV. OVERVIEW OF RELEVANT TECHNOLOGIES

A. Networking

32. Networking involves connecting multiple computers so as to support sending messages between them. Messages are broken into pieces, often called "packets," which are then routed through the network from their source to their destination. Such packets have a "header," which includes control information, such as the source's network address and the destination's network address, as well as a "payload," which is the data that is being transmitted in the packet.

33. Most modern networking protocols, including the Internet, are built using a layered architecture, which provides an organizing framework for how various protocols work. Each layer is built using services and protocols established on the lower layer and provides services and protocols for the next higher layer. For example, the protocols of the Internet are based on the following five layers:

- Layer 1: Physical. This layer specifies how to transmit bits across physical media, such as a wire or cable. It supports a service defining unique Media Access Control (MAC) addresses, which can be used by layer 2.
- Layer 2: Link. This layer is concerned with how to send messages between directly connected computers or devices.
- Layer 3: Network. This layer deals with how to route, on a best-effort basis, messages through the links of a computer network. The devices internal to the network that route the messages are typically called "routers." In the Internet, this is the layer includes the Internet Protocol (IP) that establishes

network IP addresses. This layer also supports Internet Protocol Security (IPsec), which provides authentication and encryption services for packets.

- Layer 4: Transport. This layer establishes network ports and provides a protocol (TCP) that supports sessions and guaranteed delivery of network packets.
- Layer 5: Application. This layer provides multiple protocols to support applications, which interface directly with users, including the HTTP protocol used in web browsers, the FTP protocol used for file transfers, and the SIP protocol used, e.g., for "Voice-over-IP" (VoIP) calls.

34. In addition to these layers and services, the Internet also supports a universal way of locating network resources, such as computers and data objects, using Uniform Resource Identifiers (URIs) and Uniform Resource Locators (URLs). A URI identifies a resource name and a URL is a URI that specifies a means for acting upon a network resource. For example, a URI could define a web server as "www.example.com" and a URL can specify that such a server should be accessed using the HTTP protocol as "http://www.example.com". The Doman Name System (DNS) is a hierarchical system of computers on the Internet that supports such names and provides services to map domain names, like "example.com," to IP addresses.

35. Network performance can be measured in multiple ways. For example, ***latency*** refers to the time it takes to send a packet from a source to a destination, ***bandwidth*** refers to the number of bits per second that can be

transmitted across a network connection, ***jitter*** refers to variation in packet delays, and ***congestion*** refers to the degree to which connections become overloaded with packets (which can cause packets to be delayed or lost).

36. Networks can be subdivided into components, which are often called "sub-networks" or "subnets." A ***local-area network*** (LAN) is a sub-network that includes a group of computers connected in a relatively limited area with a defined boundary, which can connect to other networks, such as the broader Internet. A LAN is often contrasted with a wide-area network (WAN), which is a geographically widespread network.

B. Firewalls and Gateways

37. One way to protect a local-area network is through the use of firewalls and/or gateways. For instance, in his book, *Computer Networks*, Tanenbaum (Ex. 2008, "Tanenbaum") explains that a firewall "provides security by carefully controlling what goes into the customer network and what comes out of it." Tanenbaum, pg. 453. Tanenbaum illustrates the functionality of a firewall as follows:

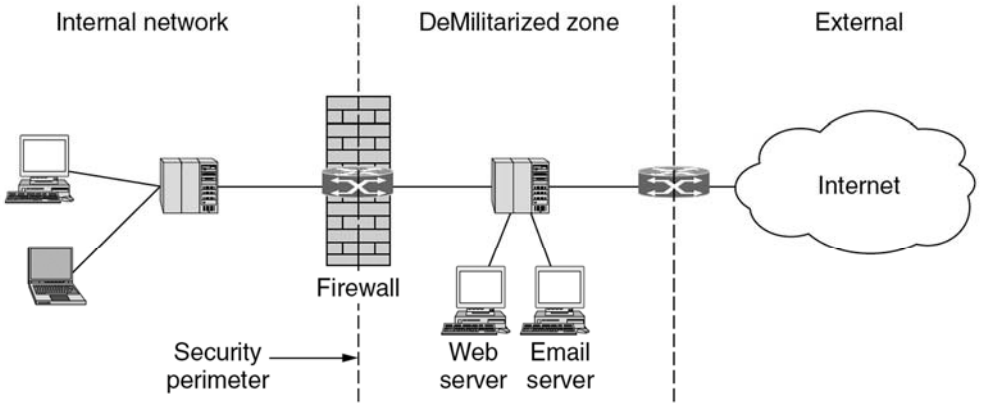


Figure 8-29. A firewall protecting an internal network.

Tanenbaum at Fig. 8-29, p. 818.

38. Tanenbaum further explains that a firewall acts as a packet filter, in that it inspects each and every incoming and outgoing packet, such that packets meeting certain rules for good packets are forwarded normally and those that fail such tests are dropped. Tanenbaum, pg. 819. In addition, Tanenbaum defines a "gateway" as "a machine that makes a connection between two or more networks and provides the necessary translation" between them, both in terms of hardware and software. Tanenbaum, pg. 28.

39. Networks can be attacked in multiple ways. For example, in a "denial-of-service" (DoS) attack, a computer on a network is inundated with so many messages, possibly including service requests (such as HTTP or FTP), that the computer cannot respond fast enough to reply to all of them. This then causes the service provided by that computer to be denied to most users. If multiple computers are used as the sources of such an attack it is also known as a distributed

denial-of-service (DDoS) attack. Such attacks are a great concern, and solutions for preventing or stopping DDoS attacks are of considerable interest. For example, my paper (J-61/C-89) on how to mark packets to trace a DDoS attack back to its sources has been cited over 300 times.

C. Packet Classification and Flow Reassembly

40. As explained in an article, "Algorithms for Packet Classification," which has been cited almost 1,000 times, "[t]he process of categorizing packets into 'flows' in an Internet router is called packet classification."[1] The abstract to this article continues:

> All packets belonging to the same flow obey a predefined rule and are processed in a similar manner by the router. For example, all packets with the same source and destination IP addresses may be defined to form a flow. Packet classification is needed for non-best-effort services, such as firewalls and quality of service; services that require the capability to distinguish and isolate traffic in different flows for suitable processing.[2]

[1] Gupta and McKeown, "Algorithms for Packet Classification," *IEEE Network*, March/April 2001, at 24. *See* Ex. 2010.

[2] *Id.*

41. One of the challenges that packet classification is meant to address is that it is common for traffic processing and filtering services to need to process traffic flows, such as FTP sessions, Telnet sessions, and HTTP sessions, but the data that comprise such flows are partitioned into separate packets. For example, a network administrator may wish to configure a network firewall to allow traffic for certain flows (such as HTTP sessions that are requested from within a protected network) while blocking other flows (such as HTTP sessions that originate outside of a protected network). By categorizing the flows to which packets belong, packet classification provides a mechanism that allows for such services.

42. The article, "Algorithms for Packet Classification," surveys a number of algorithms for packet classification, including basic search algorithms, geometric algorithms, heuristic algorithms, and hardware-specific algorithms. For example, some basic search algorithms rely on a hierarchical data structure known as a "trie," which is a digital search tree where leaf nodes represent classification outcomes and internal edges are labeled with bits or bytes. An incoming packet is classified by such a data structure by traversing the path in the data structure that corresponds to the bits/bytes that are found in the packet. For instance, a packet classification system employing a basic search algorithm might use the well-known Aho-Corasick algorithm.

43. Once packets have been classified by the flows to which they belong, a traffic filtering or analysis system often will then need to reassemble the application layer payloads of the packets from that flow. For example, the packets from an HTTP session may need to be reassembled in order to determine the full contents of a requested web page. For example, the well-known packet analysis tool, Wireshark, provides a service to reassemble TCP streams, such as those for HTTP or TLS, and explains in its documentation that "[p]rotocols such as HTTP or TLS are likely to span multiple TCP segments. The TCP protocol preference 'Allow subdissector to reassemble TCP streams' (enabled by default) makes it possible for Wireshark to collect a contiguous sequence of TCP segments and hand them over to the higher level protocol (for example, to reconstruct a full HTTP message)."[3] Ex. 2015 (7.8 Packet Reassembly) at 2. The documentation further states that reassembly of multiple packets supports full analysis of the response to an HTTP GET request: "For example, in a HTTP GET response, the requested data (e.g. an HTML page) is returned." *Id.* (7.8 Packet Reassembly) at 1. Such reassembly services come at a cost, however, in terms of memory usage and

[3] "7.8 Packet Reassembly," https://www.wireshark.org/docs/wsug_html_chunked/ChAdvReassemblySection.html, last visited April 19, 2019. *See* Ex. 2015.

processing time; hence, the documentation also states regarding the TCP reassembly feature, "Disable this preference to reduce memory and processing overhead if you are only interested in TCP sequence number analysis."

V. THE '213 PATENT

44. Centripetal develops and produces products and software solutions in the field of cybersecurity that are designed to protect computer networks against advanced cyber-attacks. A key feature of Centripetal's products and software solutions is the use of threat intelligence data as a tool to protect against sophisticated cyber threats that can compromise a computer network. The ability to integrate the most recent threat intelligence data within an existing computer network infrastructure, in a seamless manner, enables Centripetal's products and software solutions to minimize both (1) the amount of time spent by human resources and (2) the amount of computation resources deployed in order to perform similar protective measures.

45. As a means to continue its development of innovative cyber security products and solutions, Centripetal submitted and was awarded multiple patents, including the '213 Patent involved in this IPR. This patent provides a novel approach to detect sophisticated network attacks as a part of a proactive solution.

A. The Priority Date of the ’213 Patent

46. The ’213 Patent was filed on August 16, 2014. I understand that the ’213 Patent is to be evaluated under post-AIA law.

B. Person of Ordinary Skill in the Art for the ’213 Patent

47. I understand that the factors to be considered in determining the level of ordinary skill in the art to be: (1) the educational level of active workers in the field, including the named inventors of the patent; (2) the type of problems encountered in the art; (3) prior art solutions to those problems; (4) the rapidity with which innovations are made; and (5) the sophistication of the technology in the art. As mentioned above, I understand the priority date of the ’213 Patent to be August 16, 2014.

48. Based on my review of the ’213 Patent and my consideration of the above-mentioned factors, it is my opinion that a person of ordinary skill in the art (POSA) at the time of the invention of the ’213 Patent would be someone with a bachelor’s degree in computer science or related field, and either (1) two or more years of industry experience and/or (2) an advanced degree in computer science or related field. For example, the specification of the ’213 Patent discusses computer security, networking, data structures, and client-server systems. I have also considered the POSA described by Cisco, and do not find it to be materially different and my opinions are the same under that construction.

49. I believe I would qualify as a person of at least ordinary skill in the art as of the priority date of the ’213 Patent. For example, I earned a Ph.D. and published numerous articles on computer security, networking, data structures, and client-server systems before the priority date of the ’213 Patent.

C. The ’213 Patent Specification

50. The ’213 Patent is directed to providing a scalable proactive security system. ’213 Patent, 1:15-27. In particular, the ’213 Patent relates to identifying, routing, and performing packet transformation functions on network layer packets, on a packet-by-packet basis, based on application-layer packet-header information found in those network layer packets. ’213 Patent, Abstract. For example, application-layer messages utilizing the hypertext transfer protocol (HTTP) may be used to transfer information between instances of web client applications (*e.g.,* web browsers) and web server applications (*e.g.*, named websites such as www.examplewebsite.com). ’213 Patent, 7:45–59. The application-layer headers for such messages include, for example, uniform resource identifiers (URIs), values that specify the methods of for transferring data, etc. ’213 Patent, 7:56–8:3, 8:34–54.

51. When transmitted over the Internet, HTTP messages are segmented and embedded within an L3 packet (*i.e.,* a datagram) that defines, among other things, the sequence number as well as the source and destination port. These L3

packets are then embedded within an L2 packet (*i.e.*, a frame) that defines at least the source and destination IP address. One or more of packet transformation functions, can be performed on individual L2 or L3 packets based on application-layer packet header information of, for example, an HTTP packet contained therein:

> A rule may specify that **IP packets containing HTTP packets** with a GET method and transferring a resource with a particular URI should have an **accept packet transformation function** performed on them. Another rule may specify that **IP packets containing HTTP packets** with a PUT method and transferring a resource to a server with a particular URI should have a **deny packet transformation function** performed on them. Rules may specify criteria comprising values selected from five-tuple header information and/or values selected from application-layer header information.

’213 Patent at 7:60–8:3 (emphasis added). Application-layer packet-header information is structured into standardized fields at specific locations of an IP packet. Because of this feature of application-layer packet-header information, and the fact that these headers are located at the beginning of an application-layer message, the PSGs of the ’213 Patent can evaluate the header information at the network level without resorting to packet reassembly techniques typically required for application-layer content analysis. A type of packet transformation function,

referred to as a packet digest logging function can also be performed on the packets based on the application-layer packet-header information. ’213 Patent, 22:7–23:18; *see also* ’213 Patent FIG. 12. The ’213 Patent teaches that “packet transformation functions 1-N 216, 218, and 220 operate at the network layer” so a packet security gateway “may still perform packet transformation functions at the network layer” based on application-layer packet header information, which is included inside a network-layer packet. ’213 Patent at 6:39–41, claim 1.

52. That is, the “packet-by-packet” processing taught in the ’213 Patent is disclosed as occurring at the network layer, but may inspect payload data found within those individual packets. *See, e.g.*,’213 Patent at ’213 Patent at 7:60–8:3 (disclosing performing a packet-filtering rule on an IP packet containing an HTTP packet that includes specified application-layer packet-header information); *see also id.* at 21:64-22:6, 22:53-59. An advantage for this approach, of course, is that it does not require an application-layer message to be reassembled from all the packets for such a message in order for packet filtering to occur.

53. On the other hand, content analysis of the type disclosed in ACNS, while flexible, is computationally expensive and requires enormous numbers of patterns to account for the proliferation of potential malware attacks. Conversely, by specifying packet filtering rules based on five-tuple and application-layer packet-header information, the methods of the ’213 Patent can protect a network

with huge numbers of computationally inexpensive rules (*e.g.*, as compared to traditional pattern-matching rules applied to traffic flows), thereby permitting proactive network protection that scales to the volume of traffic processed by modern networks.

54. In response to determining that a L2 or L3 packet contains certain application-layer packet header information, the packet security gateway ("PSG") identifies a subset of information specified by the packet digest logging function, such as, *e.g.*, source address/port, destination address/port, URI, transport layer protocol type, etc., and generates a record for the subset of information. '213 Patent, 22:60–23:18; *see also id.,* claim 1.

55. The '213 Patent provides several diagrams illustrating network topologies for arranging packet security gateways (PSGs) and security policy management (SPM) servers. For example, Fig. 1, which I excerpt below, is illustrative of such a network topology:

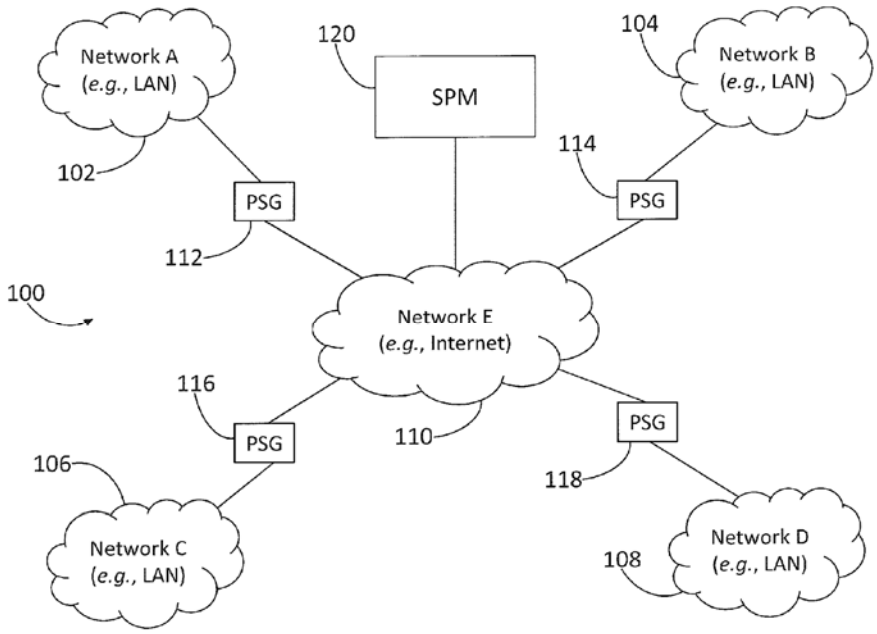


FIG. 1

'213 Patent at Fig. 1.

56. The '213 Patent also describes exemplary architectures for packet security gateways, to include components such as a processor and memory, as well as network interfaces (NIs), embedded packet transformation functions (PTFs), and a management interface (MI). For example, Fig. 2, which I excerpt below, shows such an exemplary architecture:

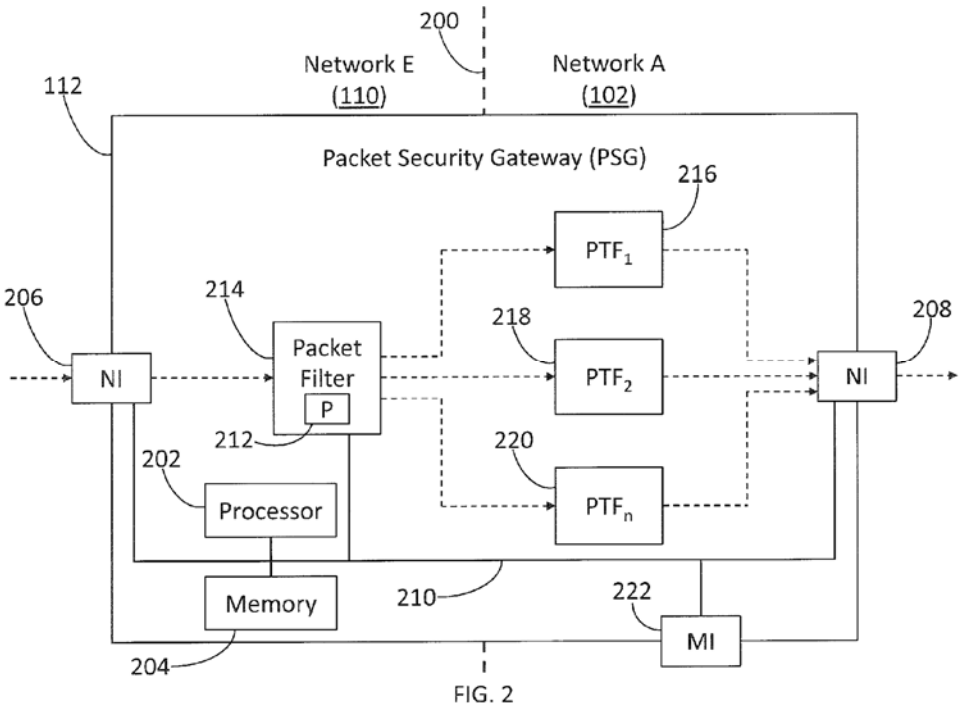


FIG. 2

'213 Patent at Fig. 2.

D. The Claims of the '213 Patent

57. The '213 Patent includes two independent claims that are included in this IPR: Claims 1 and 10. Claims 1 and 10 recite the following (subdivided according to the Petition):

'213 Patent, Claims 1 and 10
1.1. A method comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information
1.2. and a packet transformation function comprising a packet digest logging function to be performed on

packets comprising the application-layer packet-header information;[4]

1.3. receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;

1.4. identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application layer packet-header information;

1.5. performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises

1.6. identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;

1.7. generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and

1.8. reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and

1.9. routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each

[4] I note that this element is part of the "dynamic security policy" in Element 1.1.

of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.
10.1. A method comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying packet-identification criteria 10.2. and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria,[5] 10.3. wherein the packet-identification criteria comprises a Differentiated Service Code Point (DSCP) selector; 10.4. receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway; 10.5. identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria; 10.6. performing, by the packet security gateway and on a packet-by-packet basis, the packet digest logging function on each of the one or more packets corresponding to the packet-identification criteria, wherein the performing the packet digest logging function comprises: 10.7. identifying a subset of information specified by the packet digest logging function for each of the one

[5] I note that this element is part of the "dynamic security policy" in Element 10.1.

or more packets corresponding to the packet-identification criteria; 10.8. generating, for each of the one or more packets corresponding to the packet-identification criteria, a record comprising the Subset of information specified by the packet digest logging function; and 10.9. reformatting, for each of the one or more packets corresponding to the packet-identification criteria, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and 10.10. routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the packet-identification criteria in response to the performing the packet digest logging function.

58. Also, the ’213 Patent also includes several dependent claims, which I review in the element-by-element analysis given later in this declaration.

E. Claim Construction for the ’213 Patent

59. I understand that the PTAB has construed the meaning of the several claim terms for the ’213 Patent. I have applied the following constructions in my analysis:

Terms	PTAB’s Construction
rule/rules	“a condition or set of conditions that when satisfied cause a specific function to occur”
security policy management server	“a server configured to communicate a dynamic security policy to a packet gateway”
packet security gateway	“a gateway computer configured to receive packets and perform a

	packet transformation function on the packets"
packet transformation function	"operations performed on a packet"

60. I understand that all other terms are to be construed using the broadest reasonable construction in light of the specification of the patent in which they appear, and that in applying a broadest reasonable construction claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. This is the standard I used for all remaining claim terms of the '213 Patent, including the terms "packet," "dynamic security policy," and "monitoring device," which I discuss in further detail below.

VI. ALLEGED PRIOR ART

61. Dr. Jeffay's declaration relies upon the following references (collectively the "Alleged Prior Art") in an attempt to demonstrate that the challenged claims of the '213 Patent are obvious:

- Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5 ("ACNS")
- U.S. Patent No. 9,172,627 ("Kjendal")
- "An Architecture for Differentiated Services," also known as the DiffServ architecture, as defined in RFC 2475 (the "DiffServ Specification")

A. ACNS

62. ACNS (Ex. 1008) is a user guide to Version 5.5 of the ACNS system sold by Cisco Systems that was published by Cisco Systems. I have reviewed ACNS, the declaration of Eli Fuchs (Ex. 1012), and the transcript from the June 28, 2019 deposition of Eli Fuchs (Ex. 2021), and I do not believe Cisco has established the date of when Ex. 1008 was published or first available to the public. The ACNS user guide does not include a publication date. *See* Ex. 1008, generally. Cisco filed along with the Petition a declaration by Eli Fuchs stating that Ex. 1008 was available to the public at least as early as March 2008. *See* Ex. 1012 (Fuchs Decl.) at ¶ 10. However, when deposed, Mr. Fuchs stated that he did not know when Ex. 1008 was published and that he formed his opinion on the earliest date Ex. 1008 was published based on a Google search. However, Mr. Fuchs did not provide as evidence the results of the Google search that he allegedly relied upon to form his opinion. Mr. Fuchs states of his opinion:

> Q. So my question is when was it -- when was the release 5.5 user guide first available to customers?
>
> A. According to this declaration, it was at least by 2008.
>
> Q. And how do you know that it was at least by 2008?
>
> A. I generally recall that when I Googled ACNS 5.5 documentation, the Cisco website had the documentation

with the date associated with it, which led me to this declaration about a year ago.

Q. Do you have any other basis for your opinion of when the ACNS version 5.5 guide was first available other than when you did this Google search for it?

A. Not for the date because it was a long time ago.

I do know that it's general practice at Cisco that in order to release a product, you have to release the documentation with it. But I have no memory to recall exact dates. Only by Google research.

Ex. 2021 at 24:20-25:19.

Q. So the evidence -- the only evidence you provide in your declaration would be Exhibit 8; is that correct? And your testimony?

A. Yes.

Id. at 40:12-15.

63. Additionally, I attempted to access the ACNS Guide (Ex. 1008) on the Cisco website on www.cisco.com on July 3, 2019, and was able to locate the documentation for Cisco ANCS Software Version 5.5.[6] However, when I clicked on the configuration guide for Cisco ANCS Software Configuration Guide for

[6] Ex. 2017, https://www.cisco.com/c/en/us/support/application-networking-services/acns-software-version-5-5/model.html

Centrally managed Deployments, Release 5.5, the link that should have directed me to the Ex. 1008 instead led me to an End-of-Life retirement notification.[7] Accordingly, I was not able to access Ex. 1008 as of July 3, 2019. To my knowledge, Ex. 1008 is not currently publically available on Cisco website.

64. The Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5 (Ex. 1008) is a user guide describing a software solution that "expedites the delivery of strategic applications from the corporate data center to branch offices and local points of sale." Ex. 1008 at 1-1. The user guide explains that "Cisco ACNS software combines the technologies of caching, pre-positioning, and live and on-demand streaming to accelerate delivery of web applications, object files, live events, and video, enabling organizations of all sizes to reduce costs, drive up productivity, and increase revenues." *Id.*

65. The ACNS guide discloses that the Cisco ACNS software runs on the ***Cisco Content Engine*** hardware platform. It further explains that Content Engines in an ACNS network save bandwidth and protect networks by acting as ***forward proxies that authenticate, filter, and cache traffic between an organization's internal network and the Internet***. The ACNS guide also discloses that Content

[7] Ex. 2018, https://www.cisco.com/c/en/us/obsolete/application-networking-services/cisco-acns-software-version-5-5.html

Engines also perform reverse proxy caching to reduce the load on expensive back-end web servers. *Id.*

66. I understand that Dr. Jeffay is mapping the Content Engine from the ACNS guide to the "packet security gateway" of the '213 Patent. The ACNS guide discloses that "[t]he ***primary role of a Content Engine in the ACNS network is to serve client requests for content***" and that "***Content Engines also play a major role in content request routing and in channel distribution of content***." *Id.* at 1.2 (emphasis added).

67. I also understand that Dr. Jeffay is mapping the Content Distribution Managers of the ACNS guide to the Content Distribution Manager from the ACNS user guide to the "security policy management server" of the '213 Patent. The ACNS user guide discloses that "[t]he ***primary role of a Content Distribution Manager is to perform centralized content and device management***." The ACNS guide discloses a "Content Distribution Manager GUI," which allows a network administrator to specify what content is to be distributed and to whom and that "[t]he Content Distribution Manager also allows the administrator to monitor network nodes and apply changes, such as software upgrades, to groupings of nodes from a central location." *Id.* (emphasis added).

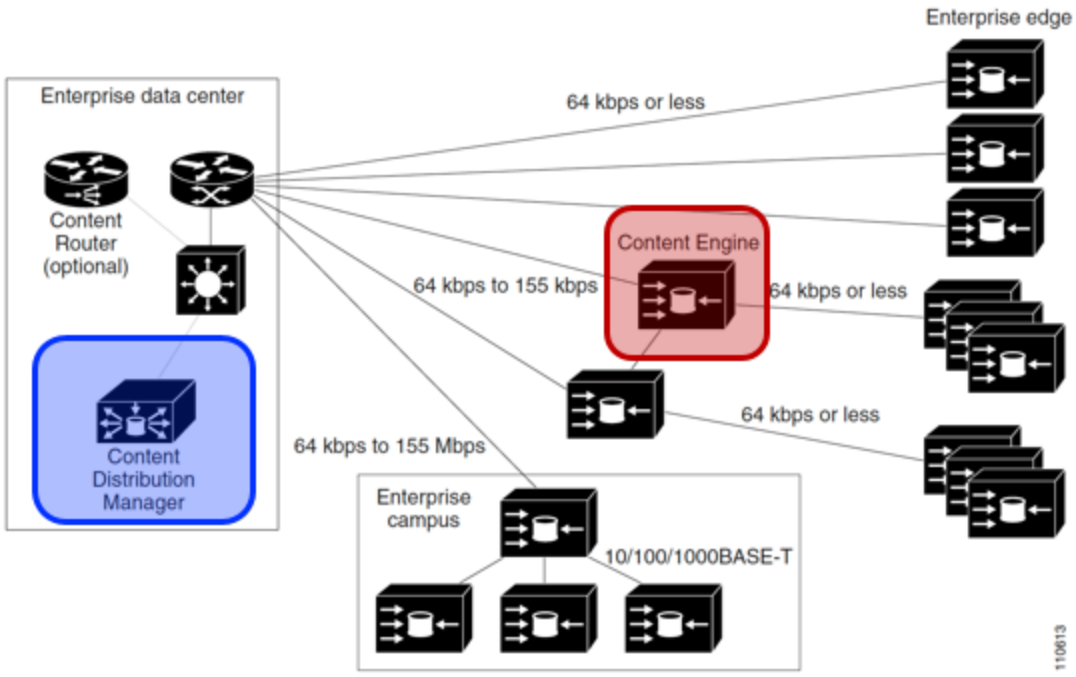
68. The ACNS guide describes a typical usage scenario with respect to a Content Engine, which supports its goal of accelerating content delivery and

optimizing bandwidth usage "by transparently caching frequently accessed content and fulfilling content requests locally rather than traversing the Internet or intranet to a distant server farm each time a request is made." *Id.* at 1-3. The ACNS guide explains this typical usage pattern as follows:

> For example, when a user requests an object from a web server, the router first sends the request to a Content Engine. If the Content Engine has a copy of the requested object in storage, the Content Engine sends the user the object. Otherwise, the Content Engine simultaneously obtains the requested objects from the web server, stores a copy of the objects (caches them), and forwards the objects on to the user.
>
> You can also configure your Content Engine as a proxy server that acts as a network gateway device, which is optimized to retrieve content on behalf of web clients. Direct proxy routing is known as nontransparent caching because the web clients and media players in the network are configured to explicitly point to the Content Engine that is acting as the proxy server.

Ex. 1008 at 1-3.

69. The ACNS guide illustrates an exemplary deployment in is Figure 1-1, which I excerpt below:



Id. at Figure 1-1, highlighting and annotations added.

70. I have annotated Figure 1-1 from the ACNS guide to highlight the placement of the Content Engine (in red) and Content Distribution Manager (in blue).

71. The ACNS guide discloses that it provides content caching, content filtering, and access control services that "[r]educe bandwidth usage by caching frequently accessed Internet content" and "[a]uthenticate, monitor, log, and control web access from end users to implement corporate policies regarding work environment and system security." *Id.* at 1-9. The ACNS guide explains that it can authenticate users, e.g., by asking the client "to provide a username and password so that it can consult an authentication, authorization, and accounting (AAA)

server, and check[] whether the client is allowed to access the web." *Id.* The ACNS guide further explains that "ACNS 5.5 software ***relies on third-party software to implement content filtering***." *Id.* at 1-10, emphasis added.

72. The ACNS guide discloses that "Content Engines accept or reject an HTTP request depending on whether the HTTP request method is supported." *Id.* at 8-23. The ACNS guide explains, for example, that "HTTP 1.1 request methods (for example, GET, HEAD, or POST) are supported by default. Nonstandard request methods, such as Web-Based Distributed Authoring and Versioning (WebDAV) are not." *Id.* The guide discloses that "[w]hen the Content Engine receives an HTTP request from a client using an unsupported method, ACNS software adds the method to the list of unsupported methods and sends an error to the client." *Id.* A POSA would understand from this disclosure (and others in the ACNS guide) that Content Engines in ACNS are processing HTTP requests as completed messages, not on a packet-by-packet basis (as is required by the claims of the '213 Patent). For example, this passage in chapter 8 regarding HTTP requests never mentions packets.

73. The general approach to content filtering and access control in ACNS, however, is fundamentally different than the packet filtering of the '213 Patent. For instance, ACNS must reassemble application-layer messages to authenticate HTTP requests or to log transactions between the Content Engines and their

clients. *See, e.g.*, Ex. 1008 at 8-23 – 8-24 (describing determine whether a content ***request*** includes a supported HTTP request method); 9-1 (describing transaction logging). Unlike ACNS, the '213 Patent describes identifying and performing packet transformation functions on a packet-by-packet basis. *See* '213 Patent, Claim 1.

74. The ACNS guide also discloses transaction logging, for instance, in chapter 19 "Using the Transaction Logs," disclosing that it can log transactions in the "Squid, Extended Squid, Apache, or customized log formats." Ex. 1008 at 19-1. The guide gives example transaction logs in the Squid format, Extended Squid format, Apache-Style format, and in a custom format. *Id.* at 19-1 - 19-3. For instance, it shows an example custom format as follows:

The following command can be entered to generate the well-known Apache Combined Log Format:

transaction-logs format custom "[%{%d}t/%{%b}t/%{%Y}t:%{%H}t:%{%M}t:%{%S}t %{%z}t] %r %s %b %{Referer}i %{User-Agent}i"

The following transaction log entry example in the Apache Combined Format is configured by using the preceding custom format string:

[11/Jan/2003:02:12:44 -0800] "GET http://www.cisco.com/swa/i/site_tour_link.gif HTTP/1.1" 200 3436 "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"

Table 19-1 Custom Format Log Format String Values

Format Token	Value
%...a	IP address of the requesting client.
%...A	IP address of the Content Engine.
%...B %...b	Bytes sent, excluding HTTP headers.

Id. at 19-3, highlighting added.

75. I have highlighted this passage to show how an ACNS transaction log entry can be customized to include a logging of the number of bytes sent, excluding HTTP headers, in the transaction. A POSA would understand, for instance, from this disclosure that the logging in ACNS is occurring with respect to complete transactions, not on a packet-by-packet basis, because the above disclosure is showing a transaction whose length (3436) in bytes is longer than the typical upper bound on the size of a packet excluding HTTP headers (which a POSA would understand to be 1500 bytes).[8] Additionally, the word "packet" never appears in chapter 19, which further evidences that the ACNS transaction log does not log information associated with packets. *See* Ex. 1008 at chapter 19.

76. ACNS does not teach a method by which information about packets are logged according to a rule within a policy. That is, ACNS does not log information about packets, let along specify "a subset" of information about packets that should be logged. Dr. Jeffay admits this omissions in paragraphs 165 of his declaration.

[8] *See, e.g.*, Ex. 2019 - "Maximum transmission unit," https://en.wikipedia.org/wiki/Maximum_transmission_unit, last visited June 17, 2019.

B. Kjendal

77. Kjendal is U.S. Patent 9,172,627, which was filed March 15, 2013, and issued October 27, 2015. Ex. 1009 ("Kjendal").

78. Kjendal teaches a function provided for the dynamic mirroring of network traffic for a variety of purposes including the identification of characteristics of the traffic. Kjendal gives multiple criteria for establishing when, what, and where to mirror the traffic. *See, e.g.*, Kjendal at Abstract.

79. Kjendal provides an illustration of the architecture of a preferred embodiment in Fig. 1, which I excerpt below:

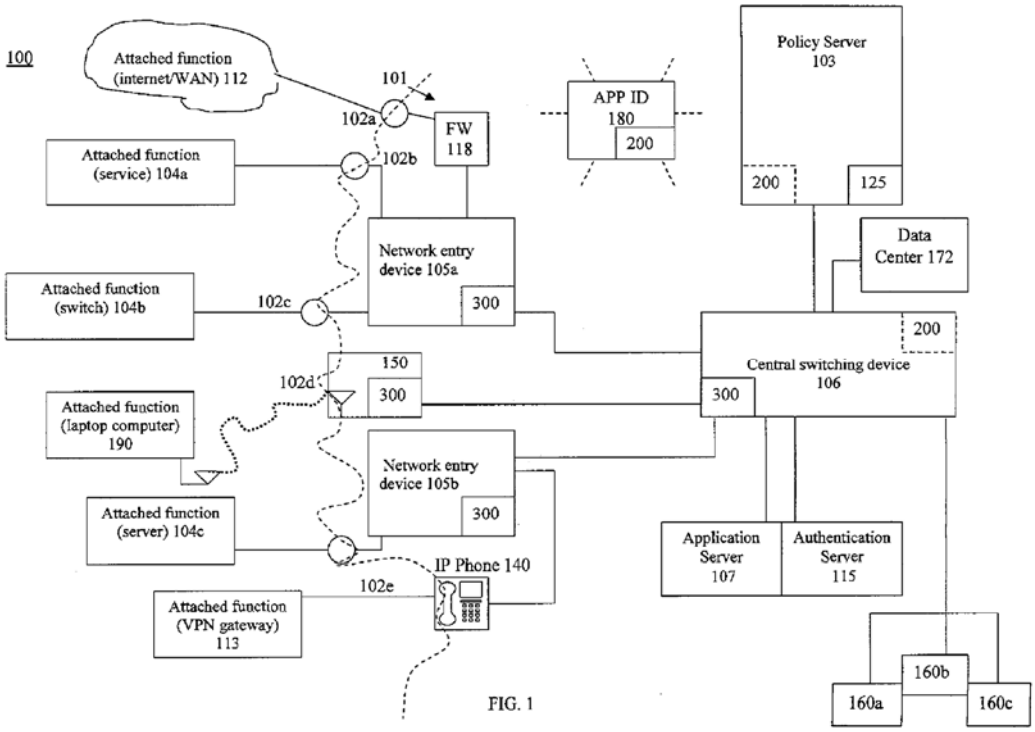


FIG. 1

80. For instance, Kjendal teaches that the network management control function 125 inside the Policy Server 103 represents network policy control,

dynamic mirror control, dynamic mirror policy control, and all other control functions taught by Kjendal. *See, e.g.*, Kjendal at 16:30-38. Kjendal also teaches that Intrusion Detection Systems (IDSs) are used to monitor the traffic associated with network sessions in an effort to detect harmful activity. *See, e.g.*, Kjendal at 4:1-3.

81. Further, Kjendal discloses that "[t]he dynamic traffic mirroring function 300 is configured to selectively mirror traffic of a flow to another device of the network infrastructure 101 including, but not limited to, a device including the application identification function 200." *Id*. at 17:3-7. Rather than disclosing a haphazard approach to mirroring, or teaching that mirroring should be added to any network device, however, Kjendal discloses that its "dynamic mirroring function enables a ***targeted approach to frame mirroring*** in order to maximize application identification effectiveness while simultaneously minimizing data that must be mirrored to an identification appliance or to any network infrastructure device configured to carry out the application identification function." *Id*. at 12:42-47, emphasis added. For example, none of the figures in Kjendal that illustrate example topologies for its embodiments (i.e., Figs. 1 and 7-10) show the dynamic mirroring function 300 installed in the firewall 118.

C. DiffServ Specification

82. DiffServ Specification is a Request for Comments (RFC) 2475, "An Architecture for Differentiated Services," by S. Blake *et al*., which has an indicated publication date of December 1998. Ex. 1011 ("DiffServ Specification").

83. DiffServ Specification defines an architecture for implementing scalable service differentiation on the Internet. Packets are classified and marked to receive a particular per-hop forwarding behavior on nodes along their path. DiffServ Specification at Abstract. A "service" in this context defines some significant characteristics of packet transmission in one direction across a set of one or more paths within a network, with those characteristics including throughput, delay, jitter, loss, or relative priorities. The architecture in DiffServ Specification is composed of a number of functional elements implemented in network nodes, including a small set of per-hop forwarding behaviors, packet classification functions, and traffic conditioning functions including metering, marking, shaping, and policing. The DiffServ Specification describes use of the DS field in IPv4 and IPv6 packet headers, with the DS field value (DS codepoint, or "DSCP field") used to mark packets to select a per-hop behavior. DiffServ Specification at 2-3.

VII. THERE IS NO MOTIVATION TO COMBINE THE CITED ALLEGED PRIOR ART

84. Dr. Jeffay opines that a POSA would be motivated to combine several alleged prior art references to result in combinations that would make the instituted claims of the '213 Patent obvious. I disagree that a POSA would be motivated to combine any of the alleged prior art references in the ways argued by Cisco, for which it cites Dr. Jeffay's declaration, for at least the reasons given below.

A. There is No Motivation to Combine ACNS, Kjendal, and Diffserv

85. Petitioner argues that a POSA would be motivated to combine ACNS, Kjendal, and Diffserv. I disagree.

1. There is no motivation to combine ACNS with Kjendal

86. A POSA would not be motivated to combine ACNS and Kjendal, for at least that reason that they teach fundamentally different techniques. Dr. Jeffay and Petitioner assert that it would be obvious to modify the transaction logging functionality of ACNS with the packet-mirroring teachings of Kjendal to "log[] only those packets identified by a rule within a dynamic security policy." *See* Ex. 1004, Jeffay Decl. ¶ 165; Petition at 30-31. Petitioner further states that "selective logging of packets, based on application-layer packet header information disclosed in Kjendal, addressed a specific problem noted in ACNS with respect the logging of HTTP authentication failures. Petition at 36. I disagree with this statement because ACNS would not base an authentication error on "application-layer

packet-header information" as Petitioner appears to assert. Instead, an authentication error would occur based on, for example, incorrect login credentials. Indeed, the transaction logging functionality of ACNS is fundamentally different than the packet mirroring system of Kjendal, for a number of reasons.

87. First, ACNS teaches transaction logging, not **packet** logging. Ex. 1008 at 19-1 – 19-22. In transaction logging, a system logs information about an entire transaction (e.g., a failure to authenticate a transaction, a time stamp of the transaction, etc.) between two devices, such as a Content Engine and its client. *Id*. at 19-19. A POSA would understand that each transaction in ACNS is typically spread over multiple packets, because transactions are often larger than the maximum transmission unit (MTU) limit of a single network-layer packet or, depending on the link-layer protocol, the maximum size of a link-layer packet (which is also known as a "frame"). This type of transaction logging in ACNS does not log information about each packet contained in the transaction, but instead logs information about the transaction as a whole, such as information about a transaction request or response.

88. Second, ACNS teaches that it can "monitor **transaction logs** in real-time for particular errors such as authentication errors," and that it can send "**transaction log messages**" to a remote server. *Id*. at 19-19, emphasis added. A POSA would recognize that ACNS authenticates clients that are attempting to

utilize the Content Engine. For example, ACNS might authenticate a client to check whether the client is allowed to access the web. Id. At 1-9 (User Authentication and Content Filtering). Using this method, ACNS could log transactions where a user authentication had failed.

89. On the other hand, and as a third reason there is no motivation to combine ACNS and Kjendal, Kjendal teaches a technique for **mirroring packets**, based on multiple criteria, which is neither transaction-based nor logging (as in ACNS). Kjendal at Abstract. Specifically, Kjendal can begin and end the mirroring of packets on the following criteria:

> [C]riteria which may generate a mirroring activity include, but are not limited to, frames of packets, the content of particular fields in a frame, flow counts, the end of a flow, a regularly timed mirroring initiation or any other conditions of interest to the network administrator can be used as conditions for establishing mirroring activities on a device of the network. In addition, events or criteria may be established for stopping the mirroring function. For example, a mirroring activity may be stopped based on the data value in a packet field, a network, regional or device specific event, a simple count of packets or other flow metric, a time out, the end of flow or based on a change in a prioritization condition (i.e., a condition has occurred wherein mirroring must be performed on a different flow that has been designated as

> being of higher priority for mirroring, particularly when the device carrying out the mirroring has limited capacity in that regard.

Kjendal at 10:1-17.

90. That is, Kjendal mirrors packets based on identifying a criterion associated with the flow of traffic (e.g., recognizing the presence of a particular field in a flow of packets). A POSA would recognize that ACNS and Kjendal teach fundamentally different approaches because Kjendal is not concerned with the information spanning over the multiple packets in a transaction, such as whether a transaction is authenticated. Instead, Kjendal is concerned with mirroring packets based on various criteria that would not identify, or be specific to, a transaction. Combining these two approaching into a workable combination would require undue experimentation and would not result in predictable results.

91. Fourth, the **packet mirroring** in Kjendal is not logging and it is not done in response to a logging action, whereas ACNS teaches **transaction logging**. Instead, Kjendal teaches that any logging it does occurs after and as a separate function from mirroring. For example, Kjendal discloses the following:

> Frames mirrored from the network devices to the identification engine 186 may also be mirrored directly to the management engine 184 for transmission to the control manager 125 or network logging or to other functions and devices.

Kjendal at 20:15-19.

92. Additionally, Petitioner asserts that "a POSA would have been motivated to implement these teachings of Kjendal into ACNS in order to only log packets that are of particular interest and thus avoid logging every packet that comes through the ACNS Content Engines, which could provide unnecessary data that may overwhelm the system." Petition at 30. However, Petitioner is creating a problem that simply does not exist within ACNS. ACNS teaches logging either all transactions or all HTTP request authorization failures. ACNS does not incur the problem of "logging every packet that comes through the ACNS Content Engine," as Petitioner asserts because it logs transactions.

About Specifying the Transaction Log Entry Type when Logging to a Remote Syslog Host

You can configure the Content Engine to send only the transactions associated with HTTP request authentication failures, or to send all of the transactions.

Typically, organizations are interested in only HTTP request authentication failures for security purposes. By monitoring these types of authentication failures in real time, it enables organizations to identify which end users failed to be authenticated through the Content Engine.

Ex. 1008, 19-21.

93. Further, absent using the '213 Patent as a guide or blueprint, there is no identified deficiency in ACNS that would motivate a POSA to look to Kjendal to fill a technological void nor a motivation to apply Kjendal-style mirroring to the Content Engines of ACNS. For example, ACNS states of its solution, "[t]ypically, organizations are interested in only HTTP request authentication failures for

security purposes." Ex. 1008 at 19-21. Indeed, ACNS does not even mention a need to log information about individual packets to satisfy its security concerns. For instance, the word "packet" appears nowhere in the ACNS chapter (19) on transaction logging. While Dr. Jeffay states that A POSA would be motivated to incorporate the packet mirroring of Kjendal into the transaction logging functionality of ACNS because there's a probability that a "packet has some indictor that it is a security threat or is objectionable" (Ex. 1004, ¶ 166), ACNS does not recognize any such deficiency or concern with packet security. Further, absent an apparent use of the '213 Patent as a blueprint, there is no motivation to apply the "targeted approach" for mirroring taught in Kjendal to install a Kjendal-style dynamic mirroring function in a Content Engine of ACNS. For example, a POSA would understand that adding mirroring to the many Content Engines in an ACNS deployment could degrade performance and Kjendal teaches away from using mirroring if it doesn't "simultaneously minimiz[e] data that must be mirrored." *See, e.g.*, Kjendal at 12:42-47.

94. Further, incorporating the teachings of Kjendal into ACNS would degrade the performance of ACNS while not improving the operating principle of ACNS. ACNS teaches transaction logging functionality to log all Content Engine transactions or all HTTP request authorization failures. Ex. 1008, 19-21. The packet mirroring technology of Kjendal, if added to ACNS' transaction logging,

would change the logging operations of ACNS. In fact, Dr. Jeffay fails to explain how ACNS would perform both transaction logging and packet logging simultaneously. Ex. 1004, ¶¶ 148, 166. A POSA would recognize that logging both packets and transactions in ACNS is wasteful, and would essentially double the storage requirements for the system (since it would require storing transactions and the packets whose payloads collectively comprise those transactions) with no discernable benefits. Further, modifying ACNS to log network packet traffic using the criteria taught by Kjendal in addition to the ACNS transaction logging would not improve the operating principle of ACNS because logging network packets in addition to transactions would not assist in ACNS' primary function of caching content and recording transaction requests and responses from web clients for content.

For at least these reasons, there is no motivation to combine ACNS with Kjendal.

1. There is No Motivation to Combine ACNS with Diffserv in the way described by Dr. Jeffay

95. Dr. Jeffay opines that a POSA would be motivated to combine ACNS with Diffserv to "enable Content Engines to classify packets and provide better-than-best effort processing to the classified packets." I disagree and would like to highlight that while the Petition alleges that the combination of ACNS and Diffserv teach logging packets identified as having a Differentiated Service Code

Point (DSCP) value, Dr. Jeffay fails explain why a POSA would be motivated to log information about packets identified by a DSCP selector. Petition at 67 (Element 10.6); Ex. 1004 at ¶¶ 237- 240.

96. A POSA would understand that the transaction logging approach of ACNS is sufficient for its purposes without the teachings of Diffserv and that Diffserv is incompatible with ACNS' logging functionality. As I discuss previously, ACNS uses **transaction logging** to log either all transactions or transactions where there has been an authorization failure. *See,* ¶¶73-76*, supra*. In my opinion, the transaction logging functionality of ACNS would not be improved by selecting packets based on the presence of a DSCP selector, for at least the same reasons I give above for why ACNS would not be improved by adding the packet mirroring taught in Kjendal. In fact, the transaction logging in ACNS is incompatible with Diffserv in the way described by Dr. Jeffay because a DSCP selector is a field in individual packets and selecting and logging packets based on this field goes against the transaction-logging approach taught in ACNS.

97. A POSA would find, therefore, that ACNS doesn't need to log packets based on the DSCP selected, as taught by Diffserv. Further, it could be counter-productive to add the teachings of Diffserv to the logging as taught by ACNS, for at least for the reason that adding packet logging to ACNS introduces would essentially double the storage required by the system, since it would require

logging every transaction and also all the packets whose payloads collectively comprise those transactions. Indeed, as Dr. Jeffay correctly points out (*e.g., see* Jeffay Decl. at paragraph 254), ACNS is already aware of Diffserv (e.g., it uses the DSCP field for non-logging functionalities at pp. 5-10 to 5-14, 10-19, 16-19 to 16-23, and 20-16 to 20-18). Tellingly, ACNS doesn't disclose using the DSCP field for transaction logging (e.g., in chapter 19 in ACNS). Indeed, as I opine elsewhere herein, a POSA would understand that a packet-based logging approach (as would be required if packet logging were based on DCSP fields in packets) is incompatible with the transaction logging taught in ACNS.

98. Further, in ACNS, facilitating differentiated services (i.e., Diffserv) is seen as a beneficial feature to enable for clients, not a security risk or an attack-recovery technique, as is taught in the '213 Patent. For example, the excerpts in ACNS cited by Dr. Jeffay that deal with DSCP fields (e.g., ACNS at pp. 5-10 to 5-14, 10-19, 16-19 to 16-23, and 20-16 to 20-18) discuss how to enable differentiated services or quality-of-service (QoS) features for Content Engines, not disable them or guard against packets with DSCP fields that are set, let alone how to use DSCP fields to recover from an attack. *See also, e.g.*, Ex. 1008, ACNS at p. 10-1 ("This chapter explains how to configure TCP stack parameters for increased performance and throughput and how to configure Type of Service (ToS) and differentiated services code point (DSCP) settings to mark content for different classes of

service"). In addition, ACNS discloses the following regarding it enabling differentiated services based on DSCP fields:

Configuring IP Differentiated Services

In the ACNS network, you can configure Content Engines, Content Routers, and Content Distribution Managers for Type of Service (ToS) or differentiated services code point (DSCP) either through the CLI of through the Content Distribution Manager GUI.

The differentiated services architecture is based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network. The class of traffic is then identified with a differentiated services (DS) code point or bit marking in the IP header. Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DS code point.

Ex. 1008, ACNS at 10-9.

99. ACNS is clearly aware of DSCP fields, but it sees them as a positive benefit for Content Engines, e.g., to quickly deliver high-priority content, not a security threat or attack remedy. Tellingly, Chapter 17 in ACNS, which deals with security threats and attacks, is silent regarding DSCP fields. It would go against the philosophy of ACNS to add DSCP checking to the techniques of chapter 17, since ACNS sees differentiated services as a positive benefit for content delivery, not a security threat or attack remedy. In my opinion, viewing DSCP fields as an indication of a possible security threat or as an attack remedy is to improperly import teachings from the '213 Patent to ACNS in apparent hindsight.

100. For at least these reasons, there is no motivation to combine ACNS with Diffserv in the way described by Dr. Jeffay; hence, there is no motivation to combine ACNS with Kjendal and Diffserv.

VIII. ELEMENT-BY-ELEMENT ANALYSIS OF THE INSTITUTED CLAIMS OF THE '213 PATENT

A. The Combination of ACNS in view of Kjendal Does Not Render Claims 1–9 of the '213 Patent Obvious

101. Claim 1 of the '213 Patent has the following elements:

1.1. A method comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises

1.2. at least one rule specifying application-layer packet-header information and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information;

1.3. receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;

1.4. identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application layer packet-header information;

1.5. performing, by the packet security gateway and on a packet-by-packet basis, the packet transformation function on each of the one or more packets comprising the application-layer packet-header information, wherein the performing the packet transformation function comprises

1.6. identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information;

> 1.7. generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function; and
>
> 1.8. reformatting, for each of the one or more packets comprising the application-layer packet-header information, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and
>
> 1.9. routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function.

102. Dr. Jeffay opines that claim 1 of the '213 Patent is rendered obvious by ACNS in view of Kjendal. I disagree. Even if there were a motivation to combine these two references (which there is not), the combination would not render obvious all the elements of claim 1.

103. Dr. Jeffay maps the Content Engine of ACNS to the "packet security gateway" of claim 1.[9] Jeffay Decl. at ¶ 147. In addition, Dr. Jeffay maps the

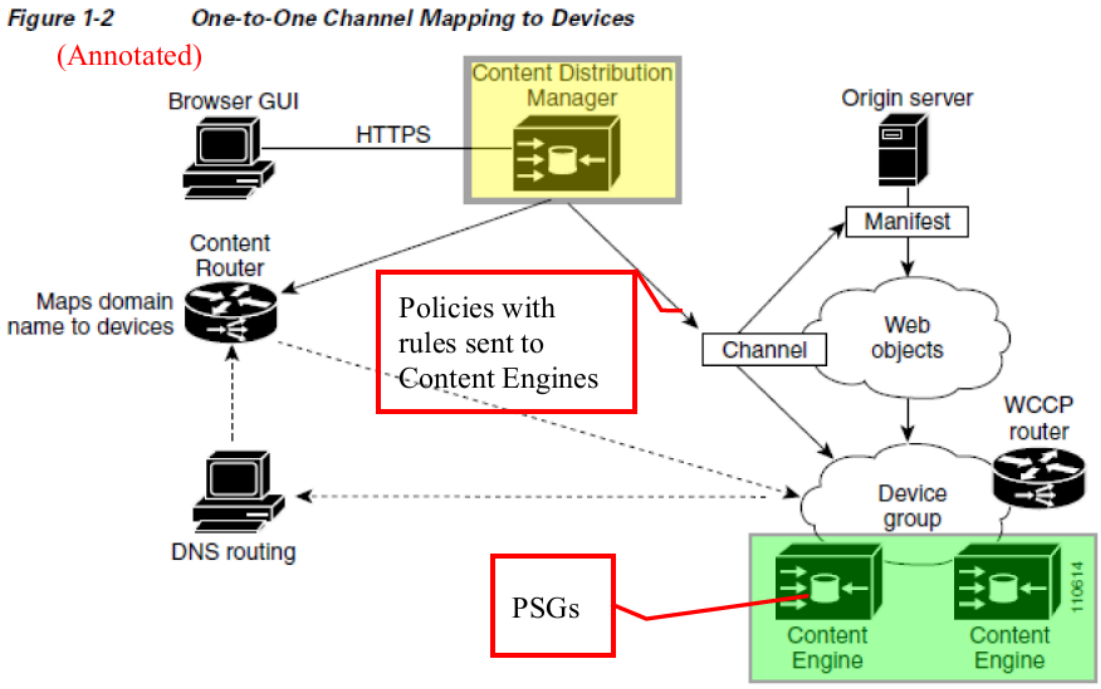
[9] Dr. Jeffay first suggests that the "Content Router" of ACNS allegedly meets the requirements of the Packet Security Gateway, which appears to be a typographical error because the remainder of Dr. Jeffay's Declaration makes clear that he believes that "Content Engine" of ACNS allegedly meets the requirements of the Packet Security Gateway. Ex. 1004 at ¶ 147.

Content Distribution Manager of ACNS to the "security policy management server" of claim 1. *Id.*

1. ACNS in view of Kjendal Does Not Disclose Element 1.1

104. I disagree with Dr. Jeffay's opinion that ACNS and Kjendal disclose "receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises at least one rule specifying application-layer packet-header information," as recited in independent claims 1 and 10.

105. Petitioner asserts that ACNS' "Content Engines (marked in green, below) represent the claimed PSGs and are associated with a Content Distribution Manager (CDM, marked in yellow) that represents the claimed SPM Server." Petition at 26. Reproduced below is the annotated ACNS Fig. 1-2, as annotated by Cisco:



EX1008, Fig. 1-2 at page 1-11 (annotated).

See Ex. 1004 at ¶ 150.

106. I disagree with Dr. Jeffay that the Content Engine is a "packet security gateway." Ex. 1004 at ¶ 150. I reviewed the deposition transcript of Eli Fuchs who submitted a declaration in this Petition (Ex. 1012) and who was a Senior Engineering Manager that led the software development team that was responsible for ACNS in the 2006 timeframe. Ex. 1012 at ¶ 2. Mr. Fuchs' testimony in combination with my analysis of ANCS forms the basis of my understanding that the Content Engine is not the "packet security gateway" because the Content Engine does ***not inspect packets*** and ***is not concerned with the security*** when it

processes requests and responses from its clients. Mr. Fuchs clearly states that the Content Engine does not inspect packets and is not concerned with security:

> Q. Does the content engine perform any security analysis on the request?
>
> A. The content engine does not perform any inspection of data within the object, no.
>
> Q. To be specific, though, does it perform any security analysis on the request itself?
>
> A. It does not.
>
> Q. Does it look at individual packets within the request?
>
> A. It does not.

Ex. 2021 at 15:2-19.

107. I agree with Mr. Fuchs testimony above and it's my understanding that the Content Engine cannot be the claimed "**packet security** gateway" because the Content Engine does not inspect individual packets and does not perform any security analysis on individual packets or request. Further, Dr. Jeffay agrees at least that the Content Engine is not able to inspect the payload of a packet for malware, further supporting my understanding that the Content Engine does not function as the claimed "packet security gateway." Ex. 2020 (6/5/2019 Jeffay Tr.) at 68:8-69:16.

108. I also disagree with Dr. Jeffay that ACNS teaches receiving dynamic security policies from a security policy management server at each of a plurality of packet security gateways. Ex. 1004 at ¶ 153. ACNS does not disclose that the Content Distribution Manager provisions any security policy to the Content Engines, as Dr. Jeffay asserts. *Id*. Instead, ACNS merely discloses that a user may add to or otherwise modify a policy already existing on a Content Engine.

109. Petitioner points to the two alleged examples of DSPs that demonstrate that the ACNS' Content Distribution Manager does not send policies to a Content Engine but is used instead to directly alter a policy already being enforced on the Content Engine. First, Petitioner first points to Chapter 8 of ACNS, which teaches using the CDM to add a rule to or modify a rule of an existing Content Engine policy. *See* Petition at 27 (citing Ex. 1004, ¶ 153; Ex. 1008 at 8-23–8-24). Chapter 8 of ACNS discloses "Adding or Modifying Additional HTTP Request Methods for the Content Engine." Ex. 1008 at p. 342 (emphasis added). A POSA would understand that adding or modifying a request method involves manually adding one HTTP request method to a plurality of request methods already configured on the Content Engine or modifying one of those already configured request methods. *See* Ex. 1008 at p. 342 ("Step 6: In the Method Name field, enter the name of the HTTP request method to be added to the list of supported methods.").

110. For example, page 8-24 shows a step-by-step guide for adding HTTP request methods. This step-by-step guide teaches that if an administrator wants to add an HTTP request method, the administrator must manually add each method to the existing policy implemented on the Content Engine. *See* Ex. 1008 at p. 8-24. Reading this section, a POSA would understand that ACNS gives a network administrator the ability to manually update an already implemented policy on a Content Engine, but ACNS does not teach that the Content Engines receive their policies from a Content Distribution Manager. Accordingly, I disagree with Petitioner's claim that chapter 8 of ACNS discloses generating a dynamic security policy. Petition at 27.

111. I also disagree with Petition's second alleged example of receiving a DSP using ACNS' command-line interface fails for the same reasons. *See* Petition at 27 (citing ACNS at C1-C27). A POSA would understand that ACNS' command-line interface simply provides the user an alternative method implementing same functionality provided by the Content Distribution Manager's GUI. For example, ACNS states:

> ***Table C-1 maps ACNS software CLI commands to the corresponding Content Distribution Manager GUI procedure***. Software CLI commands are listed in alphabetical order in the first column. The second column indicates the GUI navigation path to the device group

configuration window for each command. The third column provides a link to the GUI configuration procedure found elsewhere in this guide.

ACNS at 895 (emphasis added).

112. It's clear from the above excerpt of ACNS that the CLI only shows a table of commands that may be manually entered through the CLI to modify a setting or rule on the Content Engine. Ex. 1008 at p. 895-920. Petitioner points to the "http add-method" as allegedly being an example of a "dynamic security policy… generated at the CDM based on input by a user." Petition at 27. However, this command-line command functions exactly the same as the "Adding or Modifying Additional HTTP Request Methods for the Content Engine" cited as Petitioner's alleged first example:

http add-method *method*	Devices > Device Groups > Applications > Web > HTTP > HTTP Method	Adding or Modifying Additional HTTP Request Methods for the Content Engine, page 8-23

Ex. 1008, ACNS at 900.

113. Accordingly, I understand that Table C-1 only shows a table of commands that may be manually entered through the CLI to modify a setting or rule on the Content Engine. Petition at 27; Ex. 1008 at p. 895-920. Thus, I disagree that ACNS' teaching of CLI commands teaches a dynamic security policy provisioned to the Content Engine by the Content Distribution Manager.

114. In both of these alleged examples, a POSA would understand that the changes to the already installed policies are static, in that they will be not updated or changed automatically. Indeed, these policies are static because an administrator much manually change the settings that I discuss above to implement a change in the policy on the already installed policy. In fact, upon review of Dr. Jeffay's deposition transcript, I understand that Dr. Jeffay agrees that to be dynamic, a policy must be capable of being automatically updated. Ex. 1004, Jeffay Decl., ¶ 106 (stating that "dynamically" means "automatically"). Accordingly, it is my opinion that, ACNS does not teach or suggest automatically updating any settings and thus cannot teach or suggest a "dynamic security policy."

115. Additionally, Petitioner's argument that ACNS and Kjendal disclose a "dynamic security policy" is based on an overly broad conception of what a "dynamic security policy" is in the context of the '213 Patent. In my opinion, the word "dynamic" in the term "dynamic security policy" means that the SPM that stores the dynamic security policy and sends it to one or more PSGs that can "automatically create or alter one or more of such rules as new network addresses associated with malicious network traffic are determined." '213 Patent at 14:56–59. Dr. Jeffay's declaration indicates that he shares this opinion of what the word "dynamic" means though he incongruously concludes that the "dynamic security policy" of the '213 Patent is not, in fact, dynamic. Jeffay Decl., ¶ 106 ("In my

opinion, in the context of the '213 Patent, a dynamic security policy is not limited to a 'non-static' set of rules and may be updated dynamically (e.g., automatically) or statically (e.g., manually).").

2. ACNS and Kjendal Do Not Teach the Claimed Packet Digest Logging Function (Element [1.2])

116. I disagree with Petitioner's opinion that ACNS and Kjendal disclose "and a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information."

117. It is my opinion that ACNS performs transaction logging and does not identify and log packets on a packet-by-packet basis. I understand that Petitioner alleges that the transaction logging functionality of ACNS maps to the "packet digest logging function" of '213 Patent claims. *See* Petition at 32. Specifically, Petitioner points to Ex. 1008 at p. 19-1–19-11 ("Using the Transaction Logs.").

118. A POSA would understand that transaction logs do not create a record of individual packets. Instead, a transaction log creates a record of information derived from the transaction as a whole, which requires first reassembling the individual packets that make up the transaction and then deriving information from the transaction formed from the reassembled packets. Specifically, ACNS teaches transaction logging that creates a record of transactions between a Content Engine and its clients that meet criteria set up by a user using the GUI shown on 19-10 –

19-11, as opposed to logging information about ***each*** packet that includes application-layer packet-header information as required by Claim 1 of the '213 Patent. For example, the below example of a transaction logged by ACNS shows that a client made a request ("GET") to the Content Engine to retrieve information from the web address "http://www.cisco.com/swa/i/site_tour_link.gif." This example shows that the transaction is 3436 bytes long, which a POSA would understand is likely spread across the payloads of multiple packets because of the size of the transaction:

> [11/Jan/2003:02:12:44 -0800] "***GET http://www.cisco.com/swa/i/site_tour_link.gif*** HTTP/1.1" 200 ***3436*** "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"

Ex. 1008 at p. 19-3.

119. Further, A POSA would understand that ACNS does not log packets on a packet-by-packet basis as is required by Claim 1. Rather, as shown below, ACNS specifically states that it either logs **every** HTTP request or only those HTTP requests for which user **authentication** had failed.

About Specifying the Transaction Log Entry Type when Logging to a Remote Syslog Host

You can configure the Content Engine to send only the transactions associated with HTTP request authentication failures, or to send all of the transactions.

Typically, organizations are interested in only HTTP request authentication failures for security purposes. By monitoring these types of authentication failures in real time, it enables organizations to identify which end users failed to be authenticated through the Content Engine.

Ex. 1008 at p. 717.

120. Accordingly, It's my opinion that ACNS does not teach or suggest that the alleged "packet digest logging function" is to be performed on packets having the specified "application-layer packet-header information" or that it is part of what Petitioner contends is the dynamic security policy received from the CDM.

121. I further understand that Petitioner believes that "Kjendal teach[ing] that packets may be mirrored (i.e. sent to a network logger) based on dynamic rules specifying application-layer packet header information, such as identification of specific application types." *Id.* However, A POSA would understand that while Kjendal does disclose that one use of its technology is to mirror copies of packets to a network logger, mirroring a packet is **not** a packet digest logging function, regardless of where the mirrored packet is sent. Kjendal teaches that any logging it does occurs **after and as a separate function from mirroring**. For example, Kjendal discloses the following:

> Frames mirrored from the network devices to the identification engine 186 may also be mirrored directly to the management engine 184 for transmission to the control manager 125 or network logging or to other functions and devices.

Kjendal at 20:15-19.

122. Indeed, Kjendal's rules do not control what occurs at the network logger, let alone specify that the network logger carry out a specified packet digest logging function. Kjendal at 10:46–49.

123. That is, simply sending a copy of a packet to a device called a "network logger" is not a packet digest logging function, as claimed, which requires *inter alia* "identifying a subset of information," "generating… a record comprising the subset of information," and "reformatting… the subset of information." *See* '213 Patent at claims 1 and 10. Accordingly, even taken in combination, I conclude that ACNS and Kjendal fail to disclose receiving a dynamic security policy that includes a rule specifying (1) application-layer packet-header information and (2) a packet digest logging function to be performed upon matching application-layer packet-header information.

124. For at least these reasons, I disagree that ACNS in view of Kjendal teach or suggest "receiving… a dynamic security policy that comprises at least one rule specifying… a packet transformation function comprising a packet digest logging function to be performed on packets comprising the application-layer packet-header information," as required by claims 1 and 10.

3. ACNS in view of Kjendal Do Not Disclose Identifying Packets With Application-Layer Packet-Header Information on a Packet-by-Packet Basis (Element [1.4])

125. I disagree with Petitioner's opinion that ACNS and Kjendal disclose "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information," as recited by claim 1.

126. A POSA reading the '213 Patent would understand that the term "packet" refers to a link-layer (L2) or network-layer (L3) packet based on the OSI Model. *See* ¶ 51, *supra*. Specifically, reading the '213 Patent, I understand that claim 1 and 10 are directed to (1) receiving L2/L3 packets, (2) identifying, on a packet-by-packet basis, those packets that include application-layer packet-header information specified by a rule of a dynamic security policy, and (3) performing a packet transformation function on each identified packet, again on a packet-by-packet basis.

127. ACNS, however, does not teach identifying application-layer packet-header information in L2 or L3 packets. Rather than identifying packets that include the recited "application-layer packet-header information" on a packet-by-packet basis, ACNS must reassemble the payloads of the packets of HTTP (web) communications flows before determining whether or not a web object should be cached or whether a request for web content should be logged. In other words, the

techniques disclosed in ACNS do not include packet-filtering rules that are used to identify packets that include specified application-layer packet-header information on a "packet-by-packet basis." *Id.*

128. I further disagree with Petitioner's examples of identifying packets containing application-layer packet-header information. Petitioner's first example alleges that ACNS teaches "examin[ing] the application-layer packet-header of HTTP packets to determine whether the HTTP Request Method is supported by the Content Engine." Petition at 39-40; Ex. 1004, Jeffay Decl., ¶ 173 (citing Ex. 1008, p. 8-23). I don't dispute that ACNS identifies whether a HTTP request method is supported by the Content Engine. However, ACNS must reassemble the L2 and/or L3 packets received by the Content Engine to identify the request method. A POSA would understand that HTTP request methods such as POST are often spread over several L2 and/or L3 packets. Cisco ACNS must reassemble the L2 and L3 packets in order to identify whether a POST request method is present in the request. As shown below, ACNS looks at the entire HTTP request that is received from a client, which may be transmitted over multiple packets, to determine whether the HTTP request method is supported:

> ***Content Engines accept or reject an HTTP request depending on whether the HTTP request method is supported***. HTTP 1.1 request methods (for example, GET, HEAD, or POST) are supported by default. Nonstandard

> request methods, such as Web-Based Distributed Authoring and Versioning (WebDAV) are not.
>
> ***When the Content Engine receives an HTTP request from a client using an unsupported method***, ACNS software adds the method to the list of unsupported methods and sends an error to the client. You can use the Creating New HTTP Method for Content Engine window to add a method to the list of methods already supported by the Content Engine.

Ex. 1008 at 8-23.

129. Petitioner also states that ACNS teaches that the Content Engine identifies "packet-header information" using Internet Content Adaption Protocol ("ICAP") server functionality. Petition at 40 (citing to "rule actions" at ACNS pages 16-15 – 16-25). However, the Content Engines in ACNS are concerned with content management, which deals specifically with receiving content requests and content responses. The Content Engines are not concerned with applying rules to individual packets. *Id.; see also* Ex. 1008, ACNS at 1-2 ("[t]he primary role of a Content Engine in the ACNS network is to serve client requests for content.").

130. For at least the foregoing reasons, It's my opinion that ACNS and Kjendal, taken alone or in combination, fail to disclose "identifying, by the packet security gateway, from amongst the packets associated with the network protected

by the packet security gateway, and on a packet-by-packet basis, one or more packets comprising the application-layer packet-header information."

4. ACNS Fails to Teach Identifying a Subset of Information Specified By the Packet Digest Logging Function (Element [1.6])

131. I disagree with Petitioner's opinion that ACNS discloses "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information," as recited by claim 1.

132. Petitioner asserts that this limitation is met by ACNS' disclosure of "transaction logs." Specifically, Petitioner relies on the following example of a transaction log on page 19-1 of ACNS:

> 1012429341.115 100 **172.16.100.152** TCP_REFRESH_MISS/304 1100 **GET http://www.cisco.com/images/homepage/news.gif** - DIRECT/www.cisco.com –

Petition at 42; Ex. 1008 at 19-1.

133. The above illustration is an example of a transaction log. A POSA would understand that the information in this transaction log included various pieces of information that would be present in an entire transaction. Notably, this is not a log for an individual packet. A transaction log works by identifying and recording a subset of information in a transaction comprised of multiple individual

packets. The following example of a transaction log from ACNS further illustrates my point:

> **transaction-logs format custom "[%{%d}t/%{%b}t/%{%Y}t:%{%H}t:%{%M}t:%{%S}t %{%z}t] %r %s %b %{Referer}i %{User-Agent}i"**
>
> The following transaction log entry example in the Apache Combined Format is configured by using the preceding custom format string:
>
> [11/Jan/2003:02:12:44 -0800] "GET http://www.cisco.com/swa/i/site_tour_link.gif HTTP/1.1" 200 **3436** "http://www.cisco.com/" "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"

Ex. 1008 at 19-3

134. The transaction log example above shows that the transaction was 3,436 bytes of information, which a POSA would recognize is unlikely to have comprised a single packet because the maximum transmission unit (MTU) size of an L2/L3 packet is typically 1,500 bytes. I know that this transaction log was 3,436 bytes because the transaction log format indicates that "%b" is the variable for the size of the transaction and "3,436" is positioned in the place of the "%b" viable in the transaction log example. This example shows that (1) the transaction likely occurred over several packets, and not on a packet-by-packet basis as claim 1 recites, and (2) logging the byte size of the transactions shows that a subset of information about the transaction was logged, not a subset of information about each packet identified as having application-layer packet-header information. ACNS' disclosure of transaction logging demonstrates that ACNS logs information

at the transaction level and not of individual packets and that a transaction is often spread over multiple L2/L3 packets. Accordingly, I believe that ACNS does not teach or suggest identifying a subset of information for each packet identified as having application-layer packet-header information.

135. It's important to note that implementing a packet digest logging function as a packet transformation function permits the "information specified by the packet digest logging function" to be tailored to the condition matched by the rule, which among other benefits, enhances the ability of the '213 Patent's "[a]wareness application servers… to produce awareness information." *See* '213 Patent at 11:34–60. Because ACNS does not disclose a rule comprising a packet digest logging function that specifies the "subset of information," ACNS lacks the ability to log packet information with the level of granularity and specificity enabled by the techniques claimed in the '213 Patent.

136. Accordingly, I believe that ACNS fails to teach or suggest "identifying a subset of information specified by the packet digest logging function for each of the one or more packets comprising the application-layer packet-header information," as recited by claim 1.

5. *ACNS Fails to Teach Generating a Record for Each Packet Identifed as Having Application-Layer Packet-Header Information (Element [1.7])*

137. I disagree with Petitioner's opinion that ACNS discloses "generating, for each of the one or more packets comprising the application-layer packet-header information, a record comprising the subset of information specified by the packet digest logging function," as recited by claim 1.

138. A POSA would understand that this limitation is not met because ACNS does not perform logging at the granular level of logging information about each packet. As I have discussed above, ACNS performs transaction logging, which includes creating a record of information about a transaction as a whole, not of individual packets that may make up the more broad transaction. *See,* paras. 113-131, *supra.*

139. A POSA would understand that this limitation is directed at generating a record for each of the one or more packets that include application-layer packet header information. In my opinion, neither Dr. Jeffay nor Petitioner have cited any evidence that ACNS generates a record for each packet identified in Element [1.4]. *See, e.g.,* Jeffay Dec., ¶ 183.

6. ACNS and Kjendal Do Not Teach Routing the Identified Packets to a Monitoring Device in Response to Performing the Packet Transformation Function (Element [1.9])

140. I disagree with Petitioner's opinion that ACNS and Kjendal discloses "routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the application-layer packet-header information in response to the performing the packet transformation function." As a preliminary matter, Petitioner does not assert that ACNS meets this claim limitation. *See* Petition at 45-47.

141. I POSA would understand that Kjendal's techniques are directed to mirroring packet flows based on criteria. For example, Kjendal teaches the following traffic flow mirroring techniques:

> The dynamic traffic mirroring function can do at least one or more of: 1) mirror all or any portion of the flow, such as the first N packets, the first M fields, the first L Bytes, selected fields and one-way or bidirectional flows; 2) define flows by source address-destination address, Tuple, 5-tuple, application, etc.; and 3) transport the packets by portals to generalized or specific destinations.

Kjendal at 8:64–9:3.

142. I further understand that the Board has construed "packet transformation function" to mean "operations performed on a packet." *See* Paper 8 at p. 13. Applying the Board's construction, a POSA would understand that Kjendal does not meet this limitation. This limitation requires that the identified

packets be routed in response to applying the packet transformation function. Ex. 1001, Claim 1. However, I don't believe Kjendal teaches routing packets in response to "an operation performed on [the] packet." To the contrary, Kjendal teaches mirroring packets after they have been identified as meeting criteria. *See* Kjendal at 8:64–9:3. A POSA would understand that identifying a packet is not performing an operation on a packet within the scope of the '213 Patent. In fact, identifying ***is the precursor*** to performing an operation, such as logging. To be specific, a packet must be identified before an operation can be performed on the packet. For example, Kjendal itself distinguishes mirroring from logging and discloses mirroring done prior to logging. *See, e.g.*, Kjendal at 20:15-19.

143. Accordingly, I disagree that Kjendal's disclosure of mirroring packets that have been identified as meeting a criteria teach "routing…on a packet-by-packet basis, to a monitoring device each of the one or more packets…in response to the performing the packet transformation function," as recited by Claim 1.

B. ACNS in view of Kjendal Does Not Render Claims 2–9 of the '213 Patent Obvious

144. For at least any of the reasons given above for why claim 1 is not obvious over ACNS in view of Kjendal, claims 2–9, which depend therefrom, are also not obvious.

C. ACNS in view of Kjendal and Diffserv Specification Does Not Render Claim 10 of the '213 Patent Obvious

145. Claim 10 of the '213 Patent has the following elements:

10.1. A method comprising: receiving, by each of a plurality of packet security gateways associated with a security policy management server and from the security policy management server, a dynamic security policy that comprises

10.2. at least one rule specifying packet-identification criteria and a packet transformation function comprising a packet digest logging function to be performed on packets corresponding to the packet-identification criteria,

10.3. wherein the packet-identification criteria comprises a Differentiated Service Code Point (DSCP) selector;

10.4. receiving, by a packet security gateway of the plurality of packet security gateways, packets associated with a network protected by the packet security gateway;

10.5. identifying, by the packet security gateway, from amongst the packets associated with the network protected by the packet security gateway, and on a packet-by-packet basis, one or more packets corresponding to the packet-identification criteria;

10.6. performing, by the packet security gateway and on a packet-by-packet basis, the packet digest logging function on each of the one or more packets corresponding to the packet-identification criteria, wherein the performing the packet digest logging function comprises:

10.7. identifying a subset of information specified by the packet digest logging function for each of the one or more packets corresponding to the packet-identification criteria;

10.8. generating, for each of the one or more packets corresponding to the packet-identification criteria, a

> record comprising the Subset of information specified by the packet digest logging function; and
>
> 10.9. reformatting, for each of the one or more packets corresponding to the packet-identification criteria, the subset of information specified by the packet digest logging function in accordance with a logging system standard; and
>
> 10.10. routing, by the packet security gateway and on a packet-by-packet basis, to a monitoring device each of the one or more packets corresponding to the packet-identification criteria in response to the performing the packet digest logging function.

146. Dr. Jeffay opines that every element of claim 10 of the '213 Patent is rendered obvious by ACNS in view of Kjendal and DiffServ Specification. I disagree. Even if there were a motivation to combine all of these references (which there is not), the combination would not render obvious all the elements of claim 10.

147. Dr. Jeffay includes by reference his analysis for claim 1 of the '213 Patent. For example, this implies that he maps the Content Engine devices of ACNS to the "packet security gateway" of claim 1. In addition, Dr. Jeffay maps the Content Distribution Manager of ACNS to the "security policy management server" of claim 1. *See, e.g.*, Jeffay Decl. at ¶ 147.

148. I incorporate by reference my analysis for claim 1. That is, I reach the same conclusions as I did for claim 1 with respect to similar claim elements in

claim 10, as I explain in more detail below. Further, I incorporate by reference my analysis above for why there is no motivation to combine ACNS with Kjendal.

1. ACNS in view of Kjendal Does Not Disclose Element 10.1

149. Claim element 10.1 is identical to claim element 1.1 except it recites "packet-identification criteria" instead of "application-layer packet-header information." However, my analysis in element 1.1 applies equally to element 10.1. Element 10.1 is not disclosed by ACNS in view of Kjendal for the same reasons articulated above. I incorporate by reference my analysis regarding element 1.1.

2. ACNS in view of Kjendal Does Not Disclose Element 10.2

150. Claim element 10.2 is identical to claim element 1.2 except it recites "packet-identification criteria" instead of "application-layer packet-header information." However, my analysis in element 1.2 applies equally to element 10.2. Element 1.2 is not disclosed by ACNS in view of Kjendal for the same reasons articulated above. I incorporate by reference my analysis regarding element 1.2.

3. ACNS in view of Kjendal and DiffServ Specificaiton Does Not Disclose Element 10.3

151. I disagree with Petitioner's argument that "[t]he combination of ACNS and the DiffServ Specification teaches "wherein the packet-identification criteria comprises a Differentiated Service Code Point (DSCP) selector." Petition

at 64. It does not at least because to the extent that ACNS and DiffServ Specification disclose utilizing DSCP data, it is used for packet classification prior to the application of any security policy and not as the packet-identification criteria specified by a dynamic security policy.

152. In ACNS, facilitating differentiated services (i.e., Diffserv) is seen as a beneficial feature to enable for clients, not a security risk or an attack-recovery technique, as is taught in the 213 Patent. For example, all the sections in ACNS that deal with DSCP fields discuss how to enable differentiated services or quality-of-service (QoS) features for Content Engines, not disable them or guard against packets with DSCP fields that are set, let alone how to use DSCP fields to recover from an attack. *See*, e.g., Ex. 1008, chapters 10, 10-1 and 10-9. ACNS does not express any benefit to using DSCP to perform security services. Tellingly, Chapter 17 in ACNS deals with security threats and attacks, yet chapter 17 is silent regarding DSCP fields. So, not only would it not be obvious to add DSCP fields to the access control lists techniques of chapter 17, it would go against the philosophy of ACNS to add such checking to the techniques of chapter 17, since ACNS sees differentiated services as method for content delivery, not a security threat or attack remedy. Petitioner's argument here essentially reads out the word "security" from "security policy", "packet security gateway", and "security policy management server". *See* Petition at 64. Viewing DSCP fields as an indication of

a possible security threat or as an attack remedy is to improperly map teachings from the 213 Patent to ACNS in apparent hindsight.

153. Accordingly, ACNS in view of Diffserv Specification do not render obvious Element 10.3.

1. ACNS Does Not Disclose Element 10.7

154. Claim element 10.7 is identical to claim element 1.6 and is not disclosed by ACNS, for the same reasons articulated above. I incorporate by reference my analysis regarding element 1.6.

2. ACNS in view of Kjendal Does Not Disclose Element 10.8

155. Claim element 10.8 is identical to claim element 1.7 and is not disclosed by ACNS in view of Kjendal, for the same reasons articulated above. I incorporate by reference my analysis regarding element 1.7.

3. ACNS in view of Kjendal Does Not Disclose Element 10.10

156. Claim element 10.10 is identical to claim element 1.9 and is not disclosed by ACNS in view of Kjendal, for the same reasons articulated above. I incorporate by reference my analysis regarding element 1.9.

157. For at least any of these reasons, claim 10 of the ’213 patent is not obvious over ACNS in view of Kjendal and DiffServ Specification.

D. ACNS in view of Kjendal and Diffserv Specification Does Not Render Claims 11–16 of the '213 Patent Obvious

158. For at least any of the reasons given above for why claim 10 is not obvious over ACNS in view of Kjendal and Diffserv Specification, claims 11–16, which depend therefrom, are also not obvious.

IX. OBJECTIVE INDICIA OF NONOBVIOUSNESS

A. Recognition of a Problem, Long Felt But Unresolved Need, and Failure of Others

159. The ’213 Patent satisfied a long-felt need in the industry that others had failed to solve—namely, how to provide proactive network protection that could “scale to larger networks.” ’213 Patent at 1:20–21.

160. In 2010, the US Naval Research Laboratory hosted “Computer Network Defense/Information Assurance (CND/IA) Enabling Capability (EC) Industry Day” where Stanley Chincheck, the Director for Center for High Assurance Computer Systems, explained that previous strategies for protecting networks could not keep up with changes in the environment. Ex. 2013 (Computer Network Defense/Information Assurance Enabling Capability Industry Day) at 5. In particular, he demonstrated via the chart reproduced below that “Signature-based defense of host A/V and network firewalls are ineffective… We need new ways to frame, understand and reverse these trends.” *Id.* at 6.

Id. The failure of signature behavior based systems to keep up with emerging threats demanded new solutions. Accordingly, the long felt need for the solution provided by the '213 Patent was recognized at least as far back as 2010. *Id.*

161. The failure of others in the industry to provide proactive network protection that could scale to larger networks and meet emerging threats was recognized in the White Paper entitled "Centripetal Networks Threat Intelligence Gateway: Designed to Enable Continuous Prevention Through Intelligence-Led Enforcement." Ex. 2006 at 1 ("ESG Paper"). In particular, the ESG Paper recognized that "[t]he promise of cyber threat intelligence (CTI) for cyber-defense

has been talked about for years" and that the manual processes most enterprises have in place for using CTI "don't scale well and the forensic focus on security emergencies can cause enterprises to miss out on the benefits of proactive, preventive intelligence-based defense." *Id.* at 3. This inability for traditional systems to provide proactive, scalable network-protection services was the same problem identified in the BACKGROUND section of the '213 Patent. '213 Patent at 1:15–27.

162. The ESG Paper further acknowledged that "[t]he end goal of a threat intelligence program is defense in advance of an event" and identified "multiple challenges stand in the way of operationalizing threat intelligence in a high performance, and high-fidelity way," including "[l]ack of automation," the inability to use feeds "in a meaningful way to live network traffic and even less frequently applied inline for a protective benefit," and the ability to "turn[] CTI into actionable insight." Ex. 2006 at 4. Into this morass stepped Centripetal Networks:

> Centripetal Networks' CleanINTERNET intelligence-led managed security service using their RuleGATE enforcement point provides customized threat intelligence filtering designed to significantly reduce security event volume and workload in the enterprise. Centripetal shields the network and dynamically monitors for advanced threats using intelligence. **Centripetal's goal is nothing less than the transformation of CTI into protective action at scale. Centripetal**

> **does this by converting indicators to rules that drive actions** across a risk spectrum, i.e., **logging, content capture, mirroring, redirection**, shielding, and advanced threat detection.

Id. at 7 (emphasis added).

163. This laudatory description of Centripetal's solution to the long felt need of how to meaningfully operationalize CTI is tied to the invention disclosed and claimed in the '213 Patent. The claims of the '213 Patent are generally directed to receiving a "dynamic security policy" from a "security policy management server." *See* '213 Patent at claims 1 and 10. The "dynamic security policy" is distinguished from prior art security policies in that it is managed on a central server (the claimed SPM) and is "dynamic" in that it is automatically updated when new CTI (*i.e.* "new network addresses associated with malicious network traffic") is received at the SPM (*e.g.* from a "malicious host tracker service"). *See* '213 Patent at 3:15–21; 14:48-15:37.

164. This technique contributes to Centripetal's ability to "better manage traffic by leveraging CTI context with highly granular rules in the form of policies that can be automatically enforced." Ex. 2006 at 7. In fact, the ESG Paper describes that during its test of an embodiment of the PSG recited in the claims of the '213 Patent (*i.e.* Centripetal's Threat intelligence Gateway, RuleGATE), "[t]he intelligence was dynamically updated without loss and the results were reported in real time for live analytics." *Id.* Furthermore, the packet transformation functions

explicitly claimed in the ’213 Patent, including the packet digest logging function and routing packets meeting the specified criteria were specifically cited in the ESG Paper as helping to achieve the of “transformation of CTI into protective action at scale.” Ex. 2006 at 7.

165. The ESG Paper also praises the performance of Centripetal’s Threat Intelligence Gateway as “the highest performance network filter that ESG has tested or seen in action to date,” contrasting Centripetal’s products “with firewalls and IPS systems, which aren’t designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds.” *Id*. at 7–8. The best-in-class performance of Centripetal’s TIG owes much to the fact that the claimed dynamic security policies implement rules on a packet-by-packet basis. This technique allows the TIG to operate as a “network filter” rather than a traditional IPS that performs “deeper inspection of the application layer.” Ex. 2006 at 1.

166. Given the foregoing evidence of Centripetal’s success in solving the long felt need of operationalizing CTI, the ’213 Patent is non-obvious.

B. Industry Praise

167. Products embodying the invention claimed in the’213 Patent have received substantial industry praise. For example, the ESG Paper discussed above praised Centripetal’s TIG as having “the highest performance network filter that ESG has tested or seen in action to date.” Ex. 2006 at 8. The ESG Paper further

lauded Centripetal's TIG ability to "deliver[] more than is possible with firewalls and IPS systems":

> Simply put, Centripetal delivers more than is possible with firewalls and IPS systems, which aren't designed for—nor effective at—processing hundreds of millions of indicators from thousands of feeds. ESG watched as Centripetal Networks' Threat Intelligence Gateway solution processed over 140 Gbps of network traffic at wire speed; distributing, ingesting, synthesizing into a network policy, and enforcing over five million complex network filtering rules. Each complex filtering rule contained at-least a dozen unique fields which had to be evaluated and applied bi-directionally and without state. With intelligence enforcement there can be no presumption of insider trust so traditional filters' state assumptions are invalid.

Id. at 7.

168. Furthermore, on May 4, 2017, Gartner published its "Cool Vendors in Security for Technology and Service Providers," praising Centripetal as being "unique in its ability to instantly detect and prevent malicious network connections based on millions of threat indicators at 10-gigabit speeds." Ex. 2007 (Gardner – Cool Vendors) at 5. As described in the Cool Vendors article, Centripetal's QuickThreat Gateway "currently has the largest number of third-party threat intelligence service integrations in the network security market. It claims to be able to use up to 5 million indicators simultaneously." *Id.* Centripetal Networks was also named one of American Banker's "Top 10 FinTech Companies to Watch"

for 2014 because its Threat Intelligence Gateway, RuleGATE "has the potential to detect and deter rapidly changing cybersecurity threats on the fly." Ex. 2011 (Top 10 FirTech) at 14.

169. As discussed directly above, the salutary benefits of Centripetal's TIG discussed in the ESG Paper and the Cool Vendors article are made possible in large part by the '213 Patent's dynamic security policies, which are automatically managed and distributed by the claimed SPM, as well as its network layer packet-by-packet rule enforcement, packet digest logging function and packet transformation function for routing packets to a monitoring device.

170. Accordingly, the industry praise the products embodying the '213 Patent have received in the industry further demonstrates that the '213 Patent was not obvious.

171. I declare under penalty of perjury under the laws of the United States that the foregoing in true and correct. 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. I further declare that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed on July 5, 2019 in Irvine, California.

Dated: July 5, 2019

Michael T. Goodrich

APPENDIX A

CURRICULUM VITAE

Michael T. Goodrich

Dept. of Computer Science
Bren School of Info. & Computer Sciences
University of California, Irvine
Irvine, CA 92697-3435

E-mail: goodrich (at) acm.org
http://www.ics.uci.edu/~goodrich/
Phone: (949)824-9366
Fax: (949)824-4056

CITIZENSHIP: U.S.A.

EDUCATION

Ph.D.	1987	*Efficient Parallel Techniques for Computational Geometry* Computer Sciences, Purdue Univ. (M.J. Atallah, advisor)
M.S.	1985	Computer Sciences, Purdue Univ.
B.A.	1983	Mathematics and Computer Science, Calvin College

PROFESSIONAL EXPERIENCE

July '19 to present	Distinguished Professor, Dept. of Computer Science Univ. of California, Irvine
April '07 to June '19	Chancellor's Professor, Dept. of Computer Science Univ. of California, Irvine
July '12 to June '13	Chair, Dept. of Computer Science Univ. of California, Irvine
October '06 to June '12	Assoc. Dean for Faculty Dev., Bren School of Info. and Comp. Sci. Univ. of California, Irvine
July '01 to March '07	Professor, Dept. of Computer Science Univ. of California, Irvine
Fall '00	Visiting Professor of Computer Science Brown Univ.
July '96 to June '02	Professor of Computer Science (on leave, from July '01) Johns Hopkins Univ.
July '92 to June '96	Associate Professor of Computer Science Johns Hopkins Univ.
Spring '94	Visiting Associate Professor of Computer Science Univ. of Illinois, Urbana-Champaign
July '87 to June '92	Assistant Professor of Computer Science Johns Hopkins Univ.

RESEARCH INTERESTS

Algorithm and Data Structure Design
Information Assurance and Security
Parallel and Distributed Computing
Graph and Geometric Algorithms

HONORS AND AWARDS

- *Compere Loveless Fellowship in Computer Sciences*, Purdue Univ., 1985
- *Research Initiation Award*, National Science Foundation, 1988
- *Oraculum Award for Excellence in Teaching*, Johns Hopkins, 1993, 1994, 1995
- *ACM Recognition of Service Award*, 1996
- *Robert B. Pond, Sr. Award for Excellence in Undergraduate Teaching*, Johns Hopkins, 1998
- *Elected Senior Member*, the Institute of Electrical and Electronics Engineers (IEEE), 1999
- *Spirit of Technology Transition Award*, DARPA Dynamic Coalitions Program, 2002

- *Brown Univ. Award for Technological Innovation* (with R. Tamassia, N. Triandopoulos, D. Yao, and D. Ellis), 2006
- *ACM Distinguished Scientist*, 2006
- *2006 IEEE Computer Society Technical Achievement Award*, "for outstanding contributions to the design of parallel and distributed algorithms for fundamental combinatorial and geometric problems"
- *Fulbright Scholar*, 2007, for senior specialist service to University of Aarhus, Denmark
- *Fellow of the San Diego Supercomputer Center*, 2007
- *Fellow of the American Association for the Advancement of Science (AAAS)*, "for distinguished contributions to parallel and distributed algorithms for combinatorial and geometric problems, and excellence in teaching, academic and professional service, and textbook writing," 2007
- *Fellow of the Institute of Electrical and Electronics Engineers (IEEE)*, "for contributions to parallel and distributed algorithms for combinatorial and geometric problems," 2009
- *Fellow of the ACM*, "for contributions to data structures and algorithms for combinatorial and geometric problems," 2009
- *ICS Dean's Award for Research*, "for his contributions in the area of parallel and distributed algorithms," 2014
- *Chancellor's Award for Excellence in Fostering Undergraduate Research*, Univ. of California, Irvine, 2016
- *Faculty Mentor of the Month*, Undergraduate Research Opportunities Program (UROP), Univ. of California, Irvine, April 2016
- *Elected as a foreign member*, Royal Danish Academy of Sciences and Letters, April 2018

PUBLICATIONS

Patents and Patent Applications:

P-1. G. Ateniese, B. de Medeiros, and M.T. Goodrich, "Intermediated Delivery Scheme for Asymmetric Fair Exchange of Electronic Items," U.S. Patent Application US 2004/0073790 A1, April 15, 2004.

P-2. M.T. Goodrich and R. Tamassia, "Efficient Authenticated Dictionaries with Skip Lists and Commutative Hashing," U.S. Patent 7,257,711, August 14, 2007.

P-3. J.W. Green, J.L. Schultz, Y. Amir, and M.T. Goodrich, "High Refresh-Rate Retrieval of Freshly Published Content using Distributed Crawling," U.S. Patent 7,299,219, November 20, 2007.

P-4. R. Tamstorf, M.T. Goodrich, D. Eppstein, "Attribute Transfer Between Computer Models Including Identifying Isomorphic Regions in Polygonal Meshes," U.S. Patent 8,681,145, March 25, 2014. (also Application US 2010/0238166 A1, September 23, 2010).

P-5. N. Triandopoulos, M.T. Goodrich, D. Nguyen, O. Ohrimenko, C. Papamanthou, R. Tamassia, C.V. Lopes, "Techniques for Verifying Search Results Over a Distributed Collection," U.S. Patent, 9,152,716, October 6, 2015.

Books and Monographs:

B-1. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java*, John Wiley and Sons, Inc., 1998.

B-2. M.T. Goodrich and C.C. McGeoch, eds., *Algorithm Engineering and Experimentation*, Lecture Notes in Computer Science (LNCS), Vol. 1619, Springer-Verlag, 1999.

B-3. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Second Edition*, John Wiley and Sons, Inc., 2001.

B-4. M.T. Goodrich and R. Tamassia, *Algorithm Design: Foundations, Analysis, and Internet Examples*, John Wiley and Sons, Inc., 2002.

B-5. M.T. Goodrich and S.G. Kobourov, eds., *10th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science, Vol. 2528, Springer-Verlag, 2002.

B-6. M.T. Goodrich, R. Tamassia, and D. Mount, *Data Structures and Algorithms in C++*, John Wiley and Sons, Inc., 2004.

B-7. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Third Edition*, John Wiley and Sons, Inc., 2004.

B-8. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Fourth Edition*, John Wiley and Sons, Inc., 2006.

B-9. M.T. Goodrich and R. Tamassia, *Data Structures and Algorithms in Java, Fifth Edition*, John Wiley and Sons, Inc., 2011.

B-10. M.T. Goodrich and R. Tamassia, *Introduction to Computer Security*, Addison-Wesley, Inc., 2011.

B-11. M.T. Goodrich, R. Tamassia, and D. Mount, *Data Structures and Algorithms in C++, Second Edition*, John Wiley and Sons, Inc., 2011.

B-12. M.T. Goodrich, R. Tamassia, and M. Goldwasser, *Data Structures and Algorithms in Python*, John Wiley and Sons, Inc., 2013.

B-13. M.T. Goodrich, R. Tamassia, and M. Goldwasser, *Data Structures and Algorithms in Java, Sixth Edition*, John Wiley and Sons, Inc., 2014.

B-14. M.T. Goodrich and R. Tamassia, *Algorithm Design and Applications*, Wiley, 2015.

Book Chapters:

Ch-1. M.J. Atallah and M.T. Goodrich, "Deterministic Parallel Computational Geometry," in *Synthesis of Parallel Algorithms*, J.H. Reif, ed., Morgan Kaufmann, 497–536, 1993.

Ch-2. M.T. Goodrich, "The Grand Challenges of Geometric Computing," in *Developing a Computer Science Agenda for High-Performance Computing*, U. Vishkin, ed., ACM Press, 64–68, 1994.

Ch-3. M.T. Goodrich, "Parallel Algorithms in Geometry," *CRC Handbook of Discrete and Computational Geometry*, J.E. Goodman and J. O'Rourke, eds., CRC Press, Inc., 669–682, 1997.

Ch-4. M.T. Goodrich and K. Ramaiyer, "Geometric Data Structures," *Handbook of Computational Geometry*, J.-R. Sack and J. Urrutia, eds., Elsevier Science Publishing, 463–489, 2000.

Ch-5. M.T. Goodrich and R. Tamassia, "Simplified Analyses of Randomized Algorithms for Searching, Sorting, and Selection," *Handbook of Randomized Computing*, S. Rajasekaran, P.M. Pardalos, J.H. Reif, and J.D.P. Rolim, eds., Kluwer Academic Publishers, Vol. 1, 23–34, 2001.

Ch-6. M.T. Goodrich, "Parallel Algorithms in Geometry," *Handbook of Discrete and Computational Geometry, Second Edition*, J.E. Goodman and J. O'Rourke, eds., Chapman & Hall/CRC Press, Inc., 953–967, 2004. (Revised version of Ch-3.)

Ch-7. C. Duncan and M.T. Goodrich, "Approximate Geometric Query Structures," *Handbook of Data Structures and Applications*, Chapman & Hall/CRC Press, Inc., 26-1–26-17, 2005.

Ch-8. M.T. Goodrich, R. Tamassia, and L. Vismara, "Data Structures in JDSL," *Handbook of Data Structures and Applications*, Chapman & Hall/CRC Press, Inc., 43-1–43-22, 2005.

Ch-9. Y. Cho, L. Bao and M.T. Goodrich, "Secure Location-Based Access Control in WLAN Systems," *From Problem Toward Solution: Wireless and Sensor Networks Security*, Zhen Jiang and Yi Pan, eds., Nova Science Publishers, Inc., Chapter 17, 2007.

Ch-10. M.T. Goodrich and M.J. Nelson, "Distributed Peer-to-Peer Data Structures," *Handbook of Parallel Computing: Models, Algorithms and Applications*, R. Rajasekaran and J. Reif, eds., CRC Press, 17-1–17-17, 2008.

Ch-11. C.A. Duncan and M.T. Goodrich, "Planar Orthogonal and Polyline Drawing Algorithms," *Handbook of Graph Drawing and Visualization*, CRC Press, Inc., 223–246, 2013.

Ch-12. M.T. Goodrich, R. Tamassia, and L. Vismara, "Data Structures in JDSL," *Handbook of Data Structures and Applications*, 2nd edition, Chapman and Hall/CRC, Taylor & Francis, Inc., 43-1–43-22, 2018.

Journal Papers:

J-1. M.J. Atallah and M.T. Goodrich, "Efficient Parallel Solutions to Some Geometric Problems," *Journal of Parallel and Distributed Computing*, **3**(4), 1986, 492–507.

J-2. M.T. Goodrich, "Finding the Convex Hull of a Sorted Point Set in Parallel," *Information Processing Letters*, **26**, 1987, 173–179.

J-3. H. ElGindy and M.T. Goodrich, "Parallel Algorithms for Shortest Path Problems in Polygons," *The Visual Computer*, **3**(6), 1988, 371–378.

J-4. M.J. Atallah and M.T. Goodrich, "Parallel Algorithms For Some Functions of Two Convex Polygons," *Algorithmica*, **3**, 1988, 535–548.

J-5. M.J. Atallah, R. Cole, and M.T. Goodrich, "Cascading Divide-and-Conquer: A Technique for Designing Parallel Algorithms," *SIAM Journal on Computing*, **18**(3), 1989, 499–532.

J-6. M.T. Goodrich, "Triangulating a Polygon in Parallel," *Journal of Algorithms*, **10**, 1989, 327–351.

J-7. M.T. Goodrich and M.J. Atallah, "On Performing Robust Order Statistics in Tree-Structured Dictionary Machines," *Journal of Parallel and Distributed Computing*, **9**(1), 1990, 69–76.

J-8. M.T. Goodrich and J.S. Snoeyink, "Stabbing Parallel Segments with a Convex Polygon," *Computer Vision, Graphics and Image Processing*, **49**, 1990, 152–170.

J-9. J. Johnstone and M.T. Goodrich, "A Localized Method for Intersecting Plane Algebraic Curve Segments," *The Visual Computer*, **7**(2–3), 1991, 60–71.

J-10. M.T. Goodrich, "Intersecting Line Segments in Parallel with an Output-Sensitive Number of Processors," *SIAM Journal on Computing*, **20**(4), 1991, 737–755.

J-11. R. Cole and M.T. Goodrich, "Optimal Parallel Algorithms for Point-Set and Polygon Problems," *Algorithmica*, **7**, 1992, 3–23.

J-12. M.T. Goodrich, "A Polygonal Approach to Hidden-Line and Hidden-Surface Elimination," *Computer Vision, Graphics, and Image Processing: Graphical Models and Image Processing*, **54**(1), 1992, 1–12.

J-13. M.T. Goodrich, S. Shauck, and S. Guha, "Parallel Methods for Visibility and Shortest Path Problems in Simple Polygons," *Algorithmica*, **8**, 1992, 461–486, with addendum in *Algorithmica*, **9**, 1993, 515–516.

J-14. M.T. Goodrich, C. Ó'Dúnlaing, and C. Yap "Constructing the Voronoi Diagram of a Set of Line Segments in Parallel," *Algorithmica*, **9**, 1993, 128–141.

J-15. M.T. Goodrich, "Constructing the Convex Hull of a Partially Sorted Set of Points," *Computational Geometry: Theory and Applications*, **2**, 1993, 267–278.

J-16. M.T. Goodrich, "Constructing Arrangements Optimally in Parallel," *Discrete and*

Computational Geometry, **9**, 1993, 371–385.

J-17. M.T. Goodrich, M.J. Atallah, and M. Overmars, "Output-Sensitive Methods for Rectilinear Hidden Surface Removal," *Information and Computation*, **107**(1), 1993, 1–24.

J-18. M.J. Atallah, P. Callahan, and M.T. Goodrich, "P-Complete Geometric Problems," *Int. Journal of Computational Geometry & Applications*, **3**(4), 1993, 443–462.

J-19. M.J. Atallah, M.T. Goodrich, and S.R. Kosaraju, "Parallel Algorithms for Evaluating Sequences of Set-Manipulation Operations," *Journal of the ACM*, **41**(6), 1994, 1049–1088.

J-20. M.T. Goodrich, "Efficient Piecewise-Linear Function Approximation Using the Uniform Metric," *Discrete and Computational Geometry*, **14**, 1995, 445–462.

J-21. H. Brönnimann and M.T. Goodrich, "Almost Optimal Set Covers in Finite VC-Dimension," *Discrete and Computational Geometry*, **14**, 1995, 463–479.

J-22. M.T. Goodrich, "Planar Separators and Parallel Polygon Triangulation," *J. Computer and System Sciences*, **51**(3), 1995, 374–389.

J-23. M.T. Goodrich, M. Ghouse, and J. Bright, "Sweep Methods for Parallel Computational Geometry," *Algorithmica*, **15**(2), 1996, 126–153.

J-24. M.T. Goodrich and S.R. Kosaraju, "Sorting on a Parallel Pointer Machine with Applications to Set Expression Evaluation," *Journal of the ACM*, **43**(2), 1996, 331–361.

J-25. A. Garg, M.T. Goodrich, and R. Tamassia, "Planar Upward Tree Drawings with Optimal Area," *International Journal of Computational Geometry & Applications*, **6**(3), 1996, 333–356.

J-26. M.H. Nodine, M.T. Goodrich, and J.S. Vitter, "Blocking for External Graph Searching," *Algorithmica*, **16**(2), 1996, 181–214.

J-27. R. Cole, M.T. Goodrich, C. Ó Dúnlaing, "A Nearly Optimal Deterministic Parallel Voronoi Diagram Algorithm," *Algorithmica*, **16**, 1996, 569–617.

J-28. G. Das and M.T. Goodrich, "On the Complexity of Optimization Problems for 3-Dimensional Convex Polyhedra and Decision Trees," *Computational Geometry: Theory and Applications*, **8**, 1997, 123–137.

J-29. M.T. Goodrich and R. Tamassia, "Dynamic Ray Shooting and Shortest Paths in Planar Subdivisions via Balanced Geodesic Triangulations," *J. Algorithms*, **23**, 1997, 51–73.

J-30. M. Ghouse and M.T. Goodrich, "Fast Randomized Parallel Methods for Planar Convex Hull Construction," *Computational Geometry: Theory and Applications*, **7**, 1997, 219–235.

J-31. L.P. Chew, M.T. Goodrich, D.P. Huttenlocher, K. Kedem, J.M. Kleinberg, and D. Kravets, "Geometric Pattern Matching under Euclidean Motion," *Computational Geometry: Theory and Applications*, **7**, 1997, 113-124.

J-32. M.T. Goodrich and E.A. Ramos, "Bounded-Independence Derandomization of Geometric Partitioning with Applications to Parallel Fixed-Dimensional Linear Programming," *Discrete & Computational Geometry*, **18**(4), 1997, 397–420.

J-33. M.T. Goodrich, "An Improved Ray Shooting Method for Constructive Solid Geometry Models via Tree Contraction," *International Journal of Computational Geometry & Applications*, **8**(1), 1998, 1–23.

J-34. G. Barequet, A.J. Briggs, M.T. Dickerson, and M.T. Goodrich, "Offset-Polygon Annulus Placement Problems," *Computational Geometry: Theory and Applications*, **11**(3–4), 1998–99, 125–141.

J-35. M.T. Goodrich and R. Tamassia, "Dynamic Trees and Dynamic Point Location," *SIAM J. Comput.*, **28**(2), 1999, 612–636.

J-36. G. Barequet, S.S. Bridgeman, C.A. Duncan, M.T. Goodrich, and R. Tamassia, "GeomNet:

Geometric Computing Over the Internet," *IEEE Internet Computing*, **3**(2), 1999, 21–29.

J-37. M.T. Goodrich, J.S.B. Mitchell, and M.W. Orletsky, "Approximate Geometric Pattern Matching Under Rigid Motion," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, **21**(4), 1999, 371–379.

J-38. M.T. Goodrich, "Communication-Efficient Parallel Sorting," *SIAM Journal on Computing*, **29**(2), 1999, 416–432.

J-39. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees and Their Use for Drawing Very Large Graphs," *Journal of Graph Algorithms and Applications*, **4**(3), 2000, 19–46. Also available at www.cs.brown.edu/publications/jgaa/.

J-40. M.T. Goodrich and C.G. Wagner, "A Framework for Drawing Planar Graphs with Curves and Polylines," *Journal of Algorithms*, **37**, 2000, 399–421.

J-41. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees: Combining the Benefits of k-D Trees and Octrees," *J. Algorithms*, **38**, 2001, 303–333.

J-42. G. Barequet, M. Dickerson, and M.T. Goodrich, "Voronoi Diagrams for Polygon-Offset Distance Functions," *Discrete and Computational Geometry*, **25**(2), 2001, 271–291.

J-43. C.C. Cheng, C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Drawing Planar Graphs with Circular Arcs," *Discrete and Computational Geometry*, **25**(3), 2001, 405–418.

J-44. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "A Randomized Algorithm for Triangulating a Simple Polygon in Linear Time," *Discrete and Computational Geometry*, **26**(2), 2001, 245–265.

J-45. R. Tamassia, M.T. Goodrich, L. Vismara, M. Handy, G. Shubina, R. Cohen, B. Hudson, R.S. Baker, N. Gelfand, and U. Brandes, "JDSL: The Data Structures Library in Java," *Dr. Dobbs Journal*, **323**, 2001, 21–31.

J-46. G. Barequet, D.Z. Chen, O. Daescu, M.T. Goodrich, and J.S. Snoeyink, "Efficiently Approximating Polygonal Paths in Three and Higher Dimensions," *Algorithmica*, **33**(2), 2002, 150–167.

J-47. T. Chan, M.T. Goodrich, S.R. Kosaraju, and R. Tamassia, "Optimizing Area and Aspect Ratio in Straight-Line Orthogonal Tree Drawings," *Computational Geometry: Theory and Applications*, **23**(2), 2002, 153–162.

J-48. C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Planarity-Preserving Clustering and Embedding for Large Planar Graphs," *Computational Geometry: Theory and Applications*, **24**(2), 2003, 95–114.

J-49. A.L. Buchsbaum and M.T. Goodrich, "Three-Dimensional Layers of Maxima," *Algorithmica*, **39**, 2004, 275–286.

J-50. G. Barequet, M.T. Goodrich, and C. Riley, "Drawing Graphs with Large Vertices and Thick Edges," *J. of Graph Algorithms and Applications* (JGAA), **8**(1), 2004, 3–20.

J-51. G. Barequet, M.T. Goodrich, A. Levi-Steiner, and D. Steiner, "Contour Interpolation by Straight Skeletons," *Graphical Models* (GM), **66**(4), 2004, 245–260.

J-52. P. Gajer, M.T. Goodrich, and S.G. Kobourov, "A Multi-Dimensional Approach to Force-Directed Layouts of Large Graphs," *Computational Geometry: Theory and Applications*, **29**(1), 3–18, 2004.

J-53. G. Barequet, P. Bose, M.T. Dickerson, and M.T. Goodrich, "Optimizing a Constrained Convex Polygonal Annulus," *J. of Discrete Algorithms* (JDA), **3**(1), 1–26, 2005.

J-54. A. Bagchi, A.L. Buchsbaum, and M.T. Goodrich, "Biased Skip Lists," *Algorithmica*, **42**(1), 31–48, 2005.

J-55. M. Dickerson, D. Eppstein, M.T. Goodrich, J. Meng, "Confluent Drawings: Visualizing Non-

planar Diagrams in a Planar Way," *J. of Graph Algorithms and Applications* (JGAA), **9**(1), 31–52, 2005.

J-56. A. Bagchi, A. Chaudhary, M.T. Goodrich, C. Li, and M. Shmueli-Scheuer, "Achieving Communication Efficiency through Push-Pull Partitioning of Semantic Spaces to Disseminate Dynamic Information," *IEEE Trans. on Knowledge and Data Engineering* (TKDE), **18**(10), 1352–1367, 2006.

J-57. D. Eppstein, M.T. Goodrich, and J.Y. Meng, "Confluent Layered Drawings," *Algorithmica*, **47**(4), 439–452, 2007.

J-58. A. Bagchi, A. Chaudhary, D. Eppstein, and M.T. Goodrich, "Deterministic Sampling and Range Counting in Geometric Data Streams," *ACM Transactions on Algorithms*, **3**(2), Article 16, 2007, 18 pages.

J-59. D. Eppstein, M.T. Goodrich, and D. Hirschberg, "Improved Combinatorial Group Testing Algorithms for Real-World Problem Sizes," *SIAM Journal on Computing*, **36**(5), 1360–1375, 2007.

J-60. D. Eppstein, M.T. Goodrich, and J.Z. Sun, "Skip Quadtrees: Dynamic Data Structures for Multidimensional Point Sets," *Int. Journal on Computational Geometry and Applications*, **18**(1/2), 131–160, 2008.

J-61. M.T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback," *IEEE/ACM Transactions on Networking*, **16**(1), 15–24, 2008.

J-62. M.T. Goodrich and D.S. Hirschberg, "Improved Adaptive Group Testing Algorithms with Applications to Multiple Access Channels and Dead Sensor Diagnosis," *Journal of Combinatorial Optimization*, **15**(1), 95–121, 2008.

J-63. M.T. Goodrich, R. Tamassia, and D. Yao, "Notarized Federated ID Management and Authentication," *Journal of Computer Security*, **16**(4), 399–418, 2008.

J-64. M.T. Goodrich, "Pipelined Algorithms to Detect Cheating in Long-Term Grid Computations," *Theoretical Computer Science*, **408**, 199–207, 2008.

J-65. D. Eppstein, M.T. Goodrich, E. Kim, and R. Tamstorf, "Motorcycle Graphs: Canonical Quad Mesh Partitioning," *Computer Graphics Forum*, special issue on papers from 6th European Symp. on Geometry Processing (SGP), **27**(6), 1477–1486, 2008.

J-66. M.T. Goodrich, M. Sirivianos, J. Solis, C. Soriente, G. Tsudik, E. Uzun, "Using Audio in Secure Device Pairing," *Int. J. Security and Networks*, **4**(1/2), 57–68, 2009.

J-67. M.T. Goodrich, "On the Algorithmic Complexity of the Mastermind Game with Black-Peg Results," *Information Processing Letters*, **109**, 675–678, 2009.

J-68. D. Eppstein, M.T. Goodrich, E. Kim, and R. Tamstorf, "Approximate Topological Matching of Quad Meshes," *The Visual Computer*, **25**(8), 771–783, 2009.

J-69. D. Eppstein and M.T. Goodrich, "Succinct Greedy Geometric Routing Using Hyperbolic Geometry," *IEEE Transactions on Computers*, **60**(11), 1571–1580, 2011. Posted online Dec. 2010, IEEE Computer Society Digital Library.

J-70. D. Eppstein, M.T. Goodrich, and D. Strash, "Linear-Time Algorithms for Geometric Graphs with Sublinearly Many Edge Crossings," *SIAM Journal on Computing*, **39**(8), 3814–3829. 2010.

J-71. M.T. Goodrich, R. Tamassia, and N. Triandopoulos, "Efficient Authenticated Data Structures for Graph Connectivity and Geometric Search Problems," *Algorithmica*, **60**(3), 505–552, 2011.

J-72. D. Eppstein and M.T. Goodrich, "Straggler Identification in Round-Trip Data Streams via Newton's Identities and Invertible Bloom Filters," *IEEE Transactions on Knowledge and*

Data Engineering (TKDE), **23**(2), 297–306, 2011.

J-73. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Planar Drawings of Higher-Genus Graphs," *Journal of Graph Algorithms and Applications*, **15**(1), 7–32, 2011.

J-74. M.T. Dickerson, M.T. Goodrich, T.D. Dickerson, and Y.D. Zhuo "Round-Trip Voronoi Diagrams and Doubling Density in Geographic Networks," *Transactions on Computational Science*, M.L. Gavrilova et al. (Eds.), Vol. 14, LNCS 6970, 211–238, 2011.

J-75. M.T. Goodrich, "Randomized Shellsort: A Simple Data-Oblivious Sorting Algorithm," *Journal of the ACM*, **58**(6), Article No. 27, 2011.

J-76. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Lombardi Drawings of Graphs," *Journal of Graph Algorithms and Applications (JGAA)*, **16**(1), 85–108, 2012.

J-77. E. Wolf-Chambers, D. Eppstein, M.T. Goodrich, and M. Löffler, "Drawing Graphs in the Plane with a Prescribed Outer Face and Polynomial Area," *Journal of Graph Algorithms and Applications (JGAA)*, **16**(2), 243–259, 2012.

J-78. M.T. Goodrich, D. Nguyen, O. Ohrimenko, C. Papamanthou, R. Tamassia, N. Triandopoulos, and C.V. Lopes, "Efficient Verification of Web-Content Searching Through Authenticated Web Crawlers," *Proc. VLDB*, **5**(10):920-931, 2012.

J-79. D. Eppstein, M.T. Goodrich, D. Strash, and L. Trott, "Extended Dynamic Subgraph Statistics Using h-Index Parameterized Data Structures," *Theoretical Computer Science*, **447**, 44–52, 2012.

J-80. M.T. Goodrich, "Learning Character Strings via Mastermind Queries, With a Case Study Involving mtDNA," *IEEE Transactions on Information Theory*, **58**(11), 6726–6736, 2012.

J-81. A.U. Asuncion and M.T. Goodrich, "Nonadaptive Mastermind Algorithms for String and Vector Databases, with Case Studies," *IEEE Transactions on Knowledge and Data Engineering* (TKDE), **25**(1), 131–144, 2013.

J-82. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Drawing Trees with Perfect Angular Resolution and Polynomial Area," *Discrete & Computational Geometry*, **49**(2), 157–182, 2013.

J-83. E. Angelino, M.T. Goodrich, M. Mitzenmacher and J. Thaler, "External Memory Multimaps," *Algorithmica*, **67**(1), 23–48, 2013.

J-84. D. Eppstein, M.T. Goodrich, M. Löffler, D. Strash and L. Trott, "Category-Based Routing in Social Networks: Membership Dimension and the Small-World Phenomenon," *Theoretical Computer Science*, **514**, 96–104, 2013.

J-85. M.T. Goodrich, "Spin-the-bottle Sort and Annealing Sort: Oblivious Sorting via Round-robin Random Comparisons," *Algorithmica*, **68**(4), 835–858, 2014.

J-86. Michael J. Bannister, William E. Devanny, David Eppstein, and M.T. Goodrich, "The Galois Complexity of Graph Drawing: Why Numerical Solutions are Ubiquitous for Force-Directed, Spectral, and Circle Packing Drawings," *Journal of Graph Algorithms and Applications*, **19**(2), 619–656, 2015.

J-87. C. Duncan, D. Eppstein, M.T. Goodrich, S.G. Kobourov and M. Löffler, "Planar and Poly-Arc Lombardi Drawings," *Journal of Computational Geometry* (JoCG), **9**(1), 328–355, 2018.

Papers in Peer-Reviewed Proceedings:

C-1. M.J. Atallah and M.T. Goodrich, "Efficient Parallel Solutions to Geometric Problems," *1985 IEEE Int. Conf. on Parallel Processing (ICPP)*, 411–417. (Preliminary version of J-1.)

C-2. F. Berman, M.T. Goodrich, C. Koelbel, W. Robison, and K. Showell, "Prep-P: A Mapping Preprocessor for CHiP Computers," *1985 IEEE Int. Conf. on Parallel Processing*, 731–733.

C-3. M.J. Atallah and M.T. Goodrich, "Parallel Algorithms For Some Functions of Two Convex Polygons," *24th Allerton Conf. on Communication, Control and Computing*, 1986, 758–767. (Preliminary version of J-4.)

C-4. M.J. Atallah and M.T. Goodrich, "Efficient Plane Sweeping in Parallel," *2nd ACM Symp. on Computational Geometry* (SoCG), 1986, 216–225.

C-5. M.T. Goodrich, "A Polygonal Approach to Hidden-Line Elimination," *25th Allerton Conf. on Communication, Control, and Computing*, 1987, 849–858. (Preliminary version of J-12.)

C-6. M.J. Atallah, R. Cole, and M.T. Goodrich, "Cascading Divide-and-Conquer: A Technique for Designing Parallel Algorithms," *28th IEEE Symp. on Foundations of Computer Science* (FOCS), 1987, 151-160. (Preliminary version of J-5.)

C-7. M.J. Atallah, M.T. Goodrich, and S.R. Kosaraju, "Parallel Algorithms for Evaluating Sequences of Set-Manipulation Operations," *3rd Aegean Workshop on Computing* (AWOC), *Lecture Notes in Computer Science* (LNCS): 319, Springer-Verlag, 1988, 1–10. (Preliminary version of J-19.)

C-8. R. Cole and M.T. Goodrich, "Optimal Parallel Algorithms for Polygon and Point-Set Problems," *4th ACM Symp. on Computational Geometry* (SoCG), 1988, 201–210. (Preliminary version of J-11.)

C-9. M.T. Goodrich, "Intersecting Line Segments in Parallel with an Output-Sensitive Number of Processors," *1989 ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 127–137. (Preliminary version of J-10.)

C-10. M.T. Goodrich and S.R. Kosaraju, "Sorting on a Parallel Pointer Machine with Applications to Set Expression Evaluation," *30th IEEE Symp. on Foundations of Computer Science* (FOCS), 1989, 190–195. (Preliminary version of J-24.)

C-11. M.T. Goodrich, C. Ó'Dúnlaing, and C. Yap "Constructing the Voronoi Diagram of a Set of Line Segments in Parallel," *Lecture Notes in Computer Science 382, Algorithms and Data Structures* (WADS), Springer-Verlag, 1989, 12–23. (Preliminary version of J-14.)

C-12. M.T. Goodrich and J.S. Snoeyink, "Stabbing Parallel Segments with a Convex Polygon," *Lecture Notes in Computer Science 382, Algorithms and Data Structures* (WADS), Springer-Verlag, 1989, 231–242. (Preliminary version of J-8.)

C-13. J. Johnstone and M.T. Goodrich, "A Localized Method for Intersecting Plane Algebraic Curve Segments," *New Advances in Computer Graphics: Proc. of Computer Graphics International '89*, R.A. Earnshaw, B. Wyvel, eds., Springer-Verlag, 1989, 165–181. (Preliminary version of J-9.)

C-14. M.J. Atallah, P. Callahan, and M.T. Goodrich, "P-Complete Geometric Problems," *2nd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1990, 317–326. (Preliminary version of J-18.)

C-15. R. Cole, M.T. Goodrich, C. Ó Dúnlaing, "Merging Free Trees in Parallel for Efficient Voronoi Diagram Construction", *17th Int. Conf. on Automata, Languages, and Programming* (ICALP), 1990, 432–445. (Preliminary version of J-27.)

C-16. M.T. Goodrich, M.J. Atallah, and M. Overmars, "An Input-Size/Output-Size Trade-Off in the Time-Complexity of Rectilinear Hidden-Surface Removal", *17th Int. Conf. on Automata, Languages, and Programming* (ICALP), 1990, 689–702. (Preliminary version of J-17.)

C-17. M.T. Goodrich, M. Ghouse, and J. Bright, "Generalized Sweep Methods for Parallel Computational Geometry," *2nd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1990, 280–289. (Preliminary version of J-23.)

C-18. M.T. Goodrich, "Applying Parallel Processing Techniques to Classification Problems in

Constructive Solid Geometry," *1st ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1990, 118–128. (Preliminary version of J-33.)

C-19. M.T. Goodrich, S. Shauck, and S. Guha, "Parallel Methods for Visibility and Shortest Path Problems in Simple Polygons," *6th ACM Symp. on Computational Geometry* (SoCG), 1990, 73–82. (Preliminary version of J-13.)

C-20. M. Ghouse and M.T. Goodrich, "In-Place Techniques for Parallel Convex Hull Algorithms," *3rd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1991, 192–203. (Preliminary version of J-30.)

C-21. M.T. Goodrich, "Constructing Arrangements Optimally in Parallel," *3rd ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 1991, 169–179. (Preliminary version of J-16.)

C-22. M.T. Goodrich and R. Tamassia, "Dynamic Trees and Dynamic Point Location," *23rd ACM Symp. on Theory of Computing* (STOC), 1991, 523–533. (Preliminary version of J-35.)

C-23. M.T. Goodrich, "Using Approximation Algorithms to Design Parallel Algorithms that May Ignore Processor Allocation," *32nd IEEE Symp. on Foundations of Computer Science* (FOCS), 1991, 711–722.

C-24. M.T. Goodrich, "Planar Separators and Parallel Polygon Triangulation," *24th ACM Symp. on Theory of Computing* (STOC), 1992, 507–516. (Preliminary version of J-22.)

C-25. M.T. Goodrich, Y. Matias, U. Vishkin, "Approximate Parallel Prefix Computation and Its Applications," *7th IEEE Int. Parallel Processing Symp* (IPPS), 1993, 318–325.

C-26. M. Ghouse and M.T. Goodrich, "Experimental Evidence for the Power of Random Sampling in Practical Parallel Algorithms," *7th IEEE Int. Parallel Processing Symp* (IPPS), 1993, 549–556.

C-27. L.P. Chew, M.T. Goodrich, D.P. Huttenlocher, K. Kedem, J.M. Kleinberg, and D. Kravets, "Geometric Pattern Matching under Euclidean Motion," *5th Canadian Conf. on Computational Geometry* (CCCG), 1993, 151–156. (Preliminary version of J-31.)

C-28. M.T. Goodrich, "Geometric Partitioning Made Easier, Even in Parallel," *9th ACM Symp. on Computational Geometry* (SoCG), 1993, 73–82.

C-29. M.T. Goodrich and R. Tamassia, "Dynamic Ray Shooting and Shortest Paths via Balanced Geodesic Triangulations," *9th ACM Symp. on Computational Geometry* (SoCG), 1993, 318–327. (Preliminary version of J-29.)

C-30. A. Garg, M.T. Goodrich, and R. Tamassia, "Area-Efficient Upward Tree Drawings," *9th ACM Symp. on Computational Geometry* (SoCG), 1993, 359–368. (Preliminary version of J-25.)

C-31. M.H. Nodine, M.T. Goodrich, and J.S. Vitter, "Blocking for External Graph Searching," *12th ACM Symp. on Principles of Database Systems* (PODS), 1993, 222–232. (Preliminary version of J-26.)

C-32. E.M. Arkin, M.T. Goodrich, J.S.B. Mitchell, D. Mount, and S.S. Skiena, "Point Probe Decision Trees for Geometric Concept Classes," *Lecture Notes in Computer Science 709: Algorithms and Data Structures* (WADS), Springer-Verlag, 1993, 95–106.

C-33. M.T. Goodrich, J.J. Tsay, D.E. Vengroff, and J.S. Vitter, "External-Memory Computational Geometry," *34th IEEE Symp. on Foundations of Computer Science* (FOCS), 1993, 714–723.

C-34. M.T. Goodrich, Y. Matias, and U. Vishkin, "Optimal Parallel Approximation Algorithms for Prefix Sums and Integer Sorting," *5th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1994, 241–250.

C-35. H. Brönnimann and M.T. Goodrich, "Almost Optimal Set Covers in Finite VC-Dimension," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 293–302. (Preliminary version of J-21.)

C-36. M.T. Goodrich, "Efficient Piecewise-Linear Function Approximation Using the Uniform Metric," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 322–331. (Preliminary version of J-20.)

C-37. M.J. Atallah, M.T. Goodrich, and K. Ramaiyer, "Biased Finger Trees and Three-Dimensional Layers of Maxima," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 150–159.

C-38. M.T. Goodrich, J.S.B. Mitchell, and M.W. Orletsky, "Practical Methods for Approximate Geometric Pattern Matching under Rigid Motions," *10th ACM Symp. on Computational Geometry* (SoCG), 1994, 103–112. (Preliminary version of J-37.)

C-39. N.M. Amato, M.T. Goodrich, E.A. Ramos, "Parallel Algorithms for Higher-Dimensional Convex Hulls," *35th IEEE Symp. on Foundations of Computer Science* (FOCS), 1994, 683–694.

C-40. P.J. Tanenbaum, M.T. Goodrich, and E.R. Scheinerman, "Characterization and Recognition of Point-Halfspace and Related Orders," *2nd Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 894, Springer-Verlag, 1994, 234–245.

C-41. Y.J. Chiang, M.T. Goodrich, E.F. Grove, R. Tamassia, D.E. Vengroff, and J.S. Vitter, "External-Memory Graph Algorithms," *6th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1995, 139–149.

C-42. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "Computing Faces in Segment and Simplex Arrangements," *27th ACM Symp. on Theory of Computing* (STOC), 1995, 672–682.

C-43. P. Callahan, M.T. Goodrich, and K. Ramaiyer, "Topology B-Trees and Their Applications," *1995 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 955, Springer-Verlag, 381–392.

C-44. G. Das and M.T. Goodrich, "On the Complexity of Approximating and Illuminating Three-Dimensional Convex Polyhedra," *1995 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 955, Springer-Verlag, 74–85. (Preliminary version of J-28.)

C-45. M.T. Goodrich, "Fixed-Dimensional Parallel Linear Programming via Relative ϵ-Approximations," *7th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1996, 132–141. (Preliminary version of J-32.)

C-46. M. Chrobak, M.T. Goodrich, and R. Tamassia, "Convex Drawings of Graphs in Two and Three Dimensions," *12th ACM Symp. on Computational Geometry* (SoCG), 1996, 319–328.

C-47. M.T. Goodrich, "Communication-Efficient Parallel Sorting," *28th ACM Symp. on Theory of Computing* (STOC), 1996, 247–256. (Preliminary version of J-38.)

C-48. T. Chan, M.T. Goodrich, S.R. Kosaraju, and R. Tamassia, "Optimizing Area and Aspect Ratio in Straight-Line Orthogonal Tree Drawings," *4th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1190, Springer-Verlag, 1996, 63–75. (Preliminary version of J-47.)

C-49. M.T. Goodrich, "Randomized Fully-Scalable BSP Techniques for Multi-Searching and Convex Hull Construction," *8th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1997, 767–776.

C-50. C.A. Duncan, M.T. Goodrich, and E.A. Ramos, "Efficient Approximation and Optimization Algorithms for Computational Metrology," *8th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1997, 121–130.

C-51. M.T. Goodrich, M. Orletsky, and K. Ramaiyer, "Methods for Achieving Fast Query Times in Point Location Data Structures," *8th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1997, 757–766.

C-52. M.T. Goodrich, L.J. Guibas, J. Hershberger, P.J. Tanenbaum, "Snap Rounding Line Segments Efficiently in Two and Three Dimensions," *13th ACM Symp. on Computational Geometry* (SoCG), 1997, 284–293.

C-53. G. Barequet, S.S. Bridgeman, C.A. Duncan, M.T. Goodrich, and R. Tamassia, "Classical Computational Geometry in GeomNet," *13th ACM Symp. on Computational Geometry* (SoCG), 1997, 412–414.

C-54. G. Barequet, A. Briggs, M. Dickerson, C. Dima, and M.T. Goodrich, "Animating the Polygon-Offset Distance Function," *13th ACM Symp. on Computational Geometry* (SoCG), 1997, 479–480, and the *Video Review for the 13th ACM Symp. on Computational Geometry* (SoCG).

C-55. G. Barequet, A. Briggs, M. Dickerson, and M.T. Goodrich, "Offset-Polygon Annulus Placement Problems," *1997 Workshop on Algorithms and Data Structures* (WADS), 1997, 378–391. (Preliminary version of J-34.)

C-56. G. Barequet, M. Dickerson, and M.T. Goodrich, "Voronoi Diagrams for Polygon-Offset Distance Functions," *1997 Workshop on Algorithms and Data Structures* (WADS), 1997, 200–209. (Preliminary version of J-42.)

C-57. N. Gelfand, M.T. Goodrich, and R. Tamassia, "Teaching Data Structure Design Patterns," *29th ACM SIGCSE Technical Symp. on Computer Science Education*, 1998, 331–335.

C-58. M.T. Goodrich and R. Tamassia, "Teaching the Analysis of Algorithms with Visual Proofs," *29th ACM SIGCSE Technical Symp. on Computer Science Education*, 1998, 207–211.

C-59. G. Barequet, D.Z. Chen, O. Daescu, M.T. Goodrich, and J.S. Snoeyink, "Efficiently Approximating Polygonal Paths in Three and Higher Dimensions," *1998 ACM Symp. on Computational Geometry* (SoCG), 1998, 317–326. (Preliminary version of J-46.)

C-60. M.T. Goodrich and C.G. Wagner, "A Framework for Drawing Planar Graphs with Curves and Polylines," *6th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1547, Springer-Verlag, 1998, 153–166. (Preliminary version of J-40.)

C-61. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees and Their Use for Drawing Very Large Graphs," *6th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1547, Springer-Verlag, 1998, 111–124. (Preliminary version of J-39.)

C-62. M.T. Goodrich, M. Handy, B. Hudson, and R. Tamassia, "Abstracting Positional Information in Data Structures: Locators and Positions in JDSL," *Object-Oriented Programming, Systems, Languages & Applications (OOPSLA) '98 Technical Notes*, 1998.

C-63. M.T. Goodrich and J.G. Kloss II, "Tiered Vector: An Efficient Dynamic Array for JDSL," *Object-Oriented Programming, Systems, Languages & Applications (OOPSLA) '98 Technical Notes*, 1998.

C-64. M.T. Goodrich, M. Handy, B. Hudson, and R. Tamassia, "Accessing the Internal Organization of Data Structures in the JDSL Library," *Int. Workshop on Algorithm Engineering and Experimentation* (ALENEX), Springer-Verlag, Lecture Notes in Computer Science, Vol. 1619, 1999, 124–139.

C-65. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Balanced Aspect Ratio Trees: Combining the Benefits of k-D Trees and Octrees," *10th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 1999, 300–309. (Preliminary version of J-41.)

C-66. R.S. Baker, M. Boilen, M.T. Goodrich, R. Tamassia, and B.A. Stibel, "Testers and Visualizers for Teaching Data Structures," *30th ACM SIGCSE Technical Symp. on Computer Science Education*, 1999, 261–265.

C-67. M.T. Goodrich and R. Tamassia, "Using Randomization in the Teaching of Data Structures

and Algorithms," *30th ACM SIGCSE Technical Symp. on Computer Science Education*, 1999, 53–57. (Preliminary version of Ch-5.)

C-68. G. Barequet, C. Duncan, M.T. Goodrich, S. Kumar, M. Pop, "Efficient Perspective-Accurate Silhouette Computation," *15th ACM Symp. on Computational Geometry* (SoCG), 1999, 417–418, and the *Video Review for the 15th ACM Symp. on Computational Geometry* (SoCG).

C-69. C.C. Cheng, C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Drawing Planar Graphs with Circular Arcs," *7th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1731, Springer-Verlag, 1999, 117–126. (Preliminary version of J-43.)

C-70. C.A. Duncan, M.T. Goodrich, and S.G. Kobourov, "Planarity-Preserving Clustering and Embedding for Large Planar Graphs," *7th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1731, Springer-Verlag, 1999, 186–196. (Preliminary version of J-48.)

C-71. M.T. Goodrich and J.G. Kloss II, "Tiered Vectors: Efficient Dynamic Arrays for Rank-Based Sequences," *1999 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 1663, Springer-Verlag, 1999, 205–216.

C-72. M.T. Goodrich, "Competitive Tree-Structured Dictionaries," *11th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2000, 494–495.

C-73. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "Computing the Arrangement of Curve Segments: Divide-and-Conquer Algorithms via Sampling," *11th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2000, 705–706.

C-74. S. Bridgeman, M.T. Goodrich, S.G. Kobourov, and R. Tamassia, "PILOT: An Interactive Tool for Learning and Grading," *31st ACM SIGCSE Technical Symp. on Computer Science Education*, 2000, 139–143.

C-75. S. Bridgeman, M.T. Goodrich, S.G. Kobourov, and R. Tamassia, "SAIL: A System for Generating, Archiving, and Retrieving Specialized Assignments in LaTeX," *31st ACM SIGCSE Technical Symp. on Computer Science Education*, 2000, 300–304.

C-76. N.M. Amato, M.T. Goodrich, and E.A. Ramos, "Linear-Time Triangulation of a Simple Polygon Made Easier Via Randomization," *16th ACM Symp. on Computational Geometry* (SoCG), 2000, 201-212. (Preliminary version of J-44.)

C-77. A.L. Buchsbaum, M.T. Goodrich, and J.R. Westbrook, "Range Searching Over Tree Cross Products," *8th European Symp. on Algorithms* (ESA), Lecture Notes in Computer Science 1879, Springer-Verlag, 2000, 120–131.

C-78. C.A. Duncan, M.T. Dickerson, and M.T. Goodrich, "k-D Trees are Better When Cut on the Longest Side," *8th European Symp. on Algorithms* (ESA), Lecture Notes in Computer Science 1879, Springer-Verlag, 2000, 179–190.

C-79. P. Gajer, M.T. Goodrich, and S.G. Kobourov, "A Fast Multi-Dimensional Algorithm for Drawing Large Graphs," *8th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 1984, Springer-Verlag, 2001, 211–221. (Preliminary version of J-52.)

C-80. G. Ateniese, B. de Medeiros, and M.T. Goodrich, "TRICERT: A Distributed Certified E-mail Scheme," *Network and Distributed Systems Security Symp.* (NDSS), 2001, 47–56.

C-81. M.T. Goodrich and R. Tamassia, "Teaching Internet Algorithmics," *32nd ACM SIGCSE Technical Symp. on Computer Science Education*, 2001, 129–133.

C-82. M. Pop, G. Barequet, C.A. Duncan, M.T. Goodrich, W. Hwang, and S. Kumar, "Efficient Perspective-Accurate Silhouette Computation and Applications," *17th ACM Symp. on Computational Geometry* (SoCG), 2001, 60–68.

C-83. M.T. Goodrich and R. Tamassia, "Implementation of an Authenticated Dictionary with Skip Lists and Commutative Hashing," *DARPA Information Survivability Conf. & Exposition II*

(DISCEX), IEEE Press, 2001, 68–82.

C-84. A. Bagchi, A. Chaudhary, R. Garg, M.T. Goodrich, and V. Kumar, "Seller-Focused Algorithms for Online Auctioning," *2001 Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 2125, Springer-Verlag, 2001, 135–147.

C-85. A. Anagnostopoulos, M.T. Goodrich, R. Tamassia, "Persistent Authenticated Dictionaries and Their Applications," *Information Security Conf.* (ISC), Lecture Notes in Computer Science 2200, Springer-Verlag, 2001, 379–393.

C-86. M.T. Goodrich, R. Tamassia, and J. Hasic, "An Efficient Dynamic and Distributed Cryptographic Accumulator," *5th Information Security Conf.* (ISC), Lecture Notes in Computer Science 2433, Springer-Verlag, 2002, 372–388.

C-87. A.L. Buchsbaum and M.T. Goodrich, "Three-Dimensional Layers of Maxima," *10th European Symp. on Algorithms* (ESA), Lecture Notes in Computer Science 2461, Springer-Verlag, 2002, 257–267. (Preliminary version of J-49.)

C-88. A. Bagchi, A.L. Buchsbaum, and M.T. Goodrich, "Biased Skip Lists," *13th Int. Symp. on Algorithms and Computation* (ISAAC), Lecture Notes in Computer Science 2518, Springer-Verlag, 2002, 1–13. (Preliminary version of J-54.)

C-89. M.T. Goodrich, "Efficient Packet Marking for Large-Scale IP Traceback," *9th ACM Conf. on Computer and Communications Security* (CCS), 2002, 117–126. (Preliminary version of J-61.)

C-90. M.T. Goodrich, R. Tamassia, N. Triandopoulos, and R. Cohen, "Authenticated Data Structures for Graph and Geometric Searching," *RSA Conf.—Cryptographers' Track* (CT-RSA), Lecture Notes in Computer Science 2612, Springer-Verlag, 2003, 295–313. (Preliminary version of J-71.)

C-91. M.T. Goodrich, M. Shin, R. Tamassia, and W.H. Winsborough, "Authenticated Dictionaries for Fresh Attribute Credentials," *1st Int. Conf. on Trust Management* (iTrust), Lecture Notes in Computer Science 2692, Springer-Verlag, 2003, 332–347.

C-92. G. Barequet, M.T. Goodrich, A. Levi-Steiner, and D. Steiner, "Straight-Skeleton Based Contour Interpolation," *14th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2003, 119–127. (Preliminary version of J-51.)

C-93. G. Barequet, M.T. Goodrich, and C. Riley, "Drawing Graphs with Large Vertices and Thick Edges," *2003 Workshop and Data Structures and Algorithms* (WADS), Lecture Notes in Computer Science 2748, Springer-Verlag, 2003, 281–293. (Preliminary version of J-50.)

C-94. A. Bagchi, A. Chaudhary, M.T. Goodrich, and S. Xu, "Constructing Disjoint Paths for Secure Communication," *17th Int. Symp. on Distributed Computing* (DISC), Lecture Notes in Computer Science 2848, Springer-Verlag, 2003, 181–195.

C-95. M. Dickerson, D. Eppstein, M.T. Goodrich, J. Meng, "Confluent Drawings: Visualizing Non-planar Diagrams in a Planar Way," *11th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 2912, Springer-Verlag, 2003, 1–12. (Preliminary version of J-55.)

C-96. F. Brandenberg, D. Eppstein, M.T. Goodrich, S. Kobourov, G. Liotta, P. Mutzel, "Selected Open Problems in Graph Drawing," *11th Int. Symp. on Graph Drawing* (GD), Lecture Notes in Computer Science 2912, Springer-Verlag, 2003, 515–539.

C-97. A. Bagchi, A. Chaudhary, D. Eppstein, and M.T. Goodrich, "Deterministic Sampling and Range Counting in Geometric Data Streams," *20th ACM Symp. on Computational Geometry* (SoCG), 144–151, 2004. (Preliminary version of J-58.)

C-98. M.T. Goodrich, J.Z. Sun, and R. Tamassia, "Efficient Tree-Based Revocation in Groups of Low-State Devices," *Advances in Cryptology* (CRYPTO), Springer, Lecture Notes in Computer Science 3152, 511–527, 2004.

C-99. D. Eppstein, M.T. Goodrich, and J.Y. Meng, "Confluent Layered Drawings," *12th Int. Symp. on Graph Drawing* (GD), Springer, Lecture Notes in Computer Science 3383, 184–194, 2004. (Preliminary version of J-57.)

C-100. M.J. Atallah, K.B. Frikken, M.T. Goodrich, and R. Tamassia, "Secure Biometric Authentication for Weak Computational Devices," *9th Int. Conf. on Financial Cryptograpy and Data Security*, Springer, Lecture Notes in Computer Science 3570, 357–371, 2005.

C-101. M.T. Goodrich, "Leap-Frog Packet Linking and Diverse Key Distributions for Improved Integrity in Network Broadcasts," *IEEE Symp. on Security and Privacy* (S&P), 196–207, 2005.

C-102. D. Eppstein, M.T. Goodrich, and J.Z. Sun, "The Skip Quadtree: A Simple Dynamic Data Structure for Multidimensional Data," *21st ACM Symp. on Computational Geometry* (SoCG), 296–305, 2005. (Preliminary version of J-60.)

C-103. M.J. Atallah, M.T. Goodrich, and R. Tamassia, "Indexing Information for Data Forensics," *3rd Applied Cryptography and Network Security Conf.* (ACNS), Lecture Notes in Computer Science 3531, Springer, 206–221, 2005.

C-104. W. Du and M.T. Goodrich, "Searching for High-Value Rare Events with Uncheatable Grid Computing," *3rd Applied Cryptography and Network Security Conf.* (ACNS), Lecture Notes in Computer Science 3531, Springer, 122–137, 2005.

C-105. L. Arge, D. Eppstein, and M.T. Goodrich, "Skip-Webs: Efficient Distributed Data Structures for Multi-Dimensional Data Sets," *24th ACM Symp. on Principles of Distributed Computing* (PODC), 2005.

C-106. D. Eppstein, M.T. Goodrich, and D. Hirschberg, "Improved Combinatorial Group Testing for Real-World Problem Sizes," *Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 3608, Springer, 86–98, 2005. (Preliminary version of J-59.)

C-107. A. Chaudhary and M.T. Goodrich, "Balanced Aspect Ratio Trees Revisited," *Workshop on Algorithms and Data Structures* (WADS), Lecture Notes in Computer Science 3608, Springer, 73–85, 2005.

C-108. M.T. Goodrich, R. Tamassia, and D. Yao, "Accredited DomainKeys: A Service Architecture for Improved Email Validation," *2nd Conf. on Email and Anti-Spam* (CEAS), 1–8, 2005.

C-109. M.T. Goodrich, G.S. Lueker, and J.Z. Sun, "C-Planarity of Extrovert Clustered Graphs," *13th Int. Symp. Graph Drawing* (GD), 211–222, 2005.

C-110. D. Eppstein, M.T. Goodrich, J.Y. Meng, "Delta-Confluent Drawings," *13th Int. Symp. Graph Drawing* (GD), 165–176, 2005.

C-111. M.T. Goodrich, M.J. Nelson, and J.Z. Sun, "The Rainbow Skip Graph: A Fault-Tolerant Constant-Degree Distributed Data Structure," *17th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 384–393, 2006.

C-112. M.T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, E. Uzun, "Loud And Clear: Human-Verifiable Authentication Based on Audio," *26th IEEE Int. Conf. on Distributed Computing Systems* (ICDCS), 1–8, 2006. (Preliminary version of J-66.)

C-113. M.T. Goodrich, R. Tamassia, and D. Yao, "Notarized Federated Identity Management for Web Services," *20th IFIP WG Working Conf. on Data and Application Security* (DBSec), Springer, Lecture Notes in Computer Science, Vol. 4127, 133–147, 2006. (Preliminary version of J-63.)

C-114. M.T. Goodrich and D.S. Hirschberg, "Efficient Parallel Algorithms for Dead Sensor Diagnosis and Multiple Access Channels," *18th ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 118–127, 2006. (Preliminary version of J-62.)

C-115. Y. Cho, L. Bao, and M.T. Goodrich, "LAAC: A Location-Aware Access Control Protocol," *2006 3rd Annual Int. Conf. on Mobile and Ubiquitous Systems - Workshop on Ubiquitous Access Control* (IWUAC), 1–7, 2006.

C-116. M.B. Dillencourt, D. Eppstein, and M.T. Goodrich, "Choosing Colors for Geometric Graphs via Color Space Embeddings," *14th Int. Symp. Graph Drawing* (GD), Lecture Notes in Computer Science, Vol. 4372, Springer, 294–305, 2006.

C-117. D. Eppstein, M.T. Goodrich, and N. Sitchinava, "Guard Placement for Wireless Localization," *23rd ACM Symp. on Computational Geometry* (SoCG), 27–36, 2007.

C-118. M.T. Goodrich, C. Papamanthou, and R. Tamassia, "On the Cost of Persistence and Authentication in Skip Lists," *6th Workshop on Experimental Algorithms* (WEA), LNCS 4525, 94–107, 2007.

C-119. M.J. Atallah, M. Blanton, M.T. Goodrich, and S. Polu, "Discrepancy-Sensitive Dynamic Fractional Cascading, Dominated Maxima Searching, and 2-d Nearest Neighbors in Any Minkowski Metric," *Workshop on Algorithms and Data Structures* (WADS), LNCS, Vol. 4619, Springer, 114–126, 2007.

C-120. D. Eppstein and M.T. Goodrich, "Space-Efficient Straggler Identification in Round-Trip Data Streams via Newton's Identities and Invertible Bloom Filters," *Workshop on Algorithms and Data Structures* (WADS), LNCS, Vol. 4619, Springer, 2007, 638–649. (Preliminary version of J-72.)

C-121. M.T. Goodrich and J.Z. Sun, "Checking Value-Sensitive Data Structures in Sublinear Space," *18th Int. Symp. on Algorithms and Computation* (ISAAC), LNCS, vol. 4835, Springer, 2007, 353–364.

C-122. M.T. Goodrich, R. Tamassia, and N. Triandopoulos, "Super-Efficient Verification of Dynamic Outsourced Databases," *RSA Conf.—Cryptographers' Track* (CT-RSA), LNCS, vol. 4964, Springer, 2008, 407–424.

C-123. D. Eppstein, M.T. Goodrich, E. Kim, and R. Tamstorf, "Approximate Topological Matching of Quadrilateral Meshes," *IEEE Int. Conf. on Shape Modeling and Applications* (SMI), 2008, 83–92. (Preliminary version of J-68.)

C-124. G. Barequet, D. Eppstein, M.T. Goodrich, and A. Waxman, "Straight Skeletons of Three-Dimensional Polyhedra," *16th European Symp. on Algorithms* (ESA), LNCS, vol. 5193, 2008, 148–160.

C-125. M.T. Goodrich, C. Papamanthou, R. Tamassia, and N. Triandopoulos, "Athos: Efficient Authentication of Outsourced File Systems," *11th Information Security Conf.* (ISC), LNCS, vol. 5222, 2008, 80–96.

C-126. L. Arge, M.T. Goodrich, M. Nelson, and N. Sitchinava, "Fundamental Parallel Algorithms for Private-Cache Chip Multiprocessors," *20th ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 2008, 197–206.

C-127. D. Eppstein and M.T. Goodrich, "Succinct Greedy Graph Drawing in the Hyperbolic Plane," *16th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 5417, Springer, 2008, 14–25. (Preliminary version of J-69.)

C-128. D. Eppstein and M.T. Goodrich, "Studying (Non-Planar) Road Networks Through an Algorithmic Lens," *16th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2008, 125–134. **Best Paper Award**.

C-129. M. Dickerson and M.T. Goodrich, "Two-Site Voronoi Diagrams in Geographic Networks," *16th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2008, 439–442.

C-130. D. Eppstein, M.T. Goodrich, and D. Strash, "Linear-Time Algorithms for Geometric Graphs with Sublinearly Many Crossings," *20th ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2009, 150–159. (Preliminary version of J-70.)

C-131. M.T. Goodrich, "The Mastermind Attack on Genomic Data," *30th IEEE Symp. on Security and Privacy* (S&P), 2009, 204–218. (Preliminary version of J-80.)

C-132. W. Du, D. Eppstein, M.T. Goodrich, and G.S. Lueker, "On the Approximability of Geometric and Geographic Generalization and the Min-Max Bin Covering Problem," *Algorithms and Data Structures Symp.* (WADS), LNCS, vol. 5664, Springer, 2009, 242–253.

C-133. M.T. Goodrich, R. Tamassia, and N. Triandopoulos, J.Z. Sun, "Reliable Resource Searching in P2P Networks," *5th Int. ICST Conf. on Security and Privacy in Communication Networks* (SecureComm), Lecture Notes of ICST, vol. 19, Springer, 2009, 437–447.

C-134. C.A. Duncan, M.T. Goodrich, S.G. Kobourov, "Planar Drawings of Higher-Genus Graphs," *17th Int. Symp. on Graph Drawing* (GD), LNCS, Springer, vol. 5849, 2009, 45–56. (Preliminary version of J-73.)

C-135. D. Eppstein, M.T. Goodrich, L. Trott, "Going Off-road: Transversal Complexity in Road Networks," *17th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2009, 23–32.

C-136. M.T. Goodrich and Darren Strash, "Succinct Greedy Geometric Routing in the Euclidean Plane," *20th Int. Symp. on Algorithms and Computation* (ISAAC), LNCS, vol. 5878, Springer, 2009, 781–791.

C-137. M.T. Goodrich, "Randomized Shellsort: A Simple Oblivious Sorting Algorithm," *21st ACM-SIAM Symp. on Discrete Algorithms* (SODA), 2010, 1262–1277. (Preliminary version of J-75.)

C-138. L. Arge, M.T. Goodrich, and N. Sitchinava, "Parallel External Memory Graph Algorithms," *24th IEEE Int. Parallel & Distributed Processing Symp.* (IPDPS), 2010, 1–11.

C-139. G. Wang, T. Luo, M.T. Goodrich, W. Du, and Z. Zhu, "Bureaucratic Protocols for Secure Two-Party Sorting, Selection, and Permuting," *5th ACM Symp. on Information, Computer and Communications Security*, 2010, 226–237.

C-140. M.T. Dickerson, M.T. Goodrich, and T.D. Dickerson, "Round-Trip Voronoi Diagrams and Doubling Density in Geographic Networks," *7th Int. Symp. on Voronoi Diagrams in Science and Engineering* (ISVD), IEEE Press, 132–141, 2010. (Preliminary version of J-74.)

C-141. M.T. Dickerson, D. Eppstein, and M.T. Goodrich, "Cloning Voronoi Diagrams via Retroactive Data Structures," *18th European Symp. on Algorithms* (ESA), LNCS, vol. 6346, 2010, 362–373.

C-142. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Lombardi Drawings of Graphs," *18th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 6502, 2010, 195–207. (Preliminary version of J-76.)

C-143. E. Wolf-Chambers, D. Eppstein, M.T. Goodrich, and M. Löffler, "Drawing Graphs in the Plane with a Prescribed Outer Face and Polynomial Area," *18th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 6502, 2010, 129–140. (Preliminary version of J-77.)

C-144. C.A. Duncan, D. Eppstein, M.T. Goodrich, S. Kobourov, and M. Nöllenburg, "Drawing Trees with Perfect Angular Resolution and Polynomial Area," *18th Int. Symp. on Graph Drawing* (GD), LNCS, vol. 6502, 2010, 183–194. (Preliminary version of J-82.)

C-145. A.U. Asuncion and M.T. Goodrich, "Turning Privacy Leaks into Floods: Surreptitious Discovery of Social Network Friendships and Other Sensitive Binary Attribute Vectors," *Workshop on Privacy in the Electronic Society* (WPES), held in conjunction with the 17th

ACM Conf. on Computer and Communications Security (CCS), 2010, 21–30. (Preliminary version of J-81.)

C-146. D. Eppstein, M.T. Goodrich, D. Strash, and L. Trott, "Extended Dynamic Subgraph Statistics Using h-Index Parameterized Data Structures," *4th Annual Int. Conf. on Combinatorial Optimization and Applications* (COCOA), LNCS, vol. 6508, 2010, 128–141. (Preliminary version of J-79.)

C-147. M.T. Goodrich and D. Strash, "Priority Range Trees," *21st Int. Symp. on Algorithms and Computation* (ISAAC), LNCS, vol. 6506, 2010, 97–108.

C-148. D. Eppstein, M.T. Goodrich, R. Tamassia, "Privacy-Preserving Data-Oblivious Geometric Algorithms for Geographic Data," *18th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems* (GIS), 2010, 13–22.

C-149. M.T. Goodrich, "Spin-the-bottle Sort and Annealing Sort: Oblivious Sorting via Round-robin Random Comparisons," *8th Workshop on Analytic Algorithmics and Combinatorics* (ANALCO), in conjunction with the ACM-SIAM Symp. on Discrete Algorithms (SODA), 2011. (Preliminary version of J-85.)

C-150. M.T. Goodrich and F. Kerschbaum, "Privacy-Enhanced Reputation-Feedback Methods to Reduce Feedback Extortion in Online Auctions," *ACM Conf. on Data and Application Security and Privacy (CODASPY)*, 2011, 273–282.

C-151. M.T. Goodrich, "Data-Oblivious External-Memory Algorithms for the Compaction, Selection, and Sorting of Outsourced Data," *23rd ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 2011, 379–388.

C-152. M.T. Goodrich and M. Mitzenmacher, "Brief Announcement: Large-Scale Multimaps," *23rd ACM Symp. on Parallelism in Algorithms and Architectures* (SPAA), 2011, 259–260.

C-153. D. Eppstein, M.T. Goodrich, F. Uyeda, and G. Varghese, "What's the Difference? Efficient Set Synchronization without Prior Context," *SIGCOMM* 218–229, 2011.

C-154. D. Eppstein, M.T. Goodrich, and M. Löffler, "Tracking Moving Objects with Few Handovers," *Algorithms and Data Structures Symp.* (WADS), 362–373, LNCS, vol. 6844, 2011.

C-155. M.T. Goodrich and M. Mitzenmacher, "Privacy-Preserving Access of Outsourced Data via Oblivious RAM Simulation," *38th Int. Colloquium on Automata, Languages and Programming (ICALP)*, LNCS, vol. 6756, 2011, 576–587.

C-156. M.T. Goodrich and P. Pszona, "External-Memory Network Analysis Algorithms for Naturally Sparse Graphs," *European Symp. on Algorithms (ESA)*, LNCS, vol. 6942, 664–676, 2011.

C-157. C. Duncan, D. Eppstein, M.T. Goodrich, S.G. Kobourov and M. Löffler, "Planar and Poly-Arc Lombardi Drawings," *Int. Symp. Graph Drawing (GD)*, LNCS, vol. 7034, 308–319, 2011. (Preliminary version of J-87.)

C-158. R. Chernobelskiy, K. Cunningham, M.T. Goodrich, S.G. Kobourov and L. Trott, "Force-Directed Lombardi-Style Graph Drawing," *Int. Symp. Graph Drawing (GD)*, LNCS, vol. 7034, 320–331, 2011.

C-159. M.T. Goodrich and M. Mitzenmacher, "Invertible Bloom Lookup Tables," *49th Allerton Conf. on Communication, Control, and Computing*, IEEE Press, **invited paper**, 2011.

C-160. M.T. Goodrich, M. Mitzenmacher, O. Ohrimenko, and R. Tamassia, "Oblivious RAM Simulation with Efficient Worst-Case Access Overhead," *ACM Cloud Computing Security Workshop (CCSW)*, in conjunction with the 17th ACM Conf. on Computer and Communications Security (CCS), 95–100, 2011.

C-161. M.T. Goodrich and J.A. Simons, "Fully Retroactive Approximate Range and Nearest Neighbor Searching," *22nd Int. Symp. on Algorithms and Computation (ISAAC)*, Springer, LNCS, vol. 7074, 292–301, 2011.

C-162. E. Angelino, M.T. Goodrich, M. Mitzenmacher and J. Thaler, "External Memory Multimaps," *22nd Int. Symp. on Algorithms and Computation (ISAAC)*, Springer, LNCS, vol. 7074, 384–394, 2011. (Preliminary version of J-83.)

C-163. M.T. Goodrich, N. Sitchinava, and Q. Zhang, "Sorting, Searching, and Simulation in the MapReduce Framework," *22nd Int. Symp. on Algorithms and Computation (ISAAC)*, Springer, LNCS, vol. 7074, 374–383, 2011.

C-164. D. Eppstein, M.T. Goodrich, M. Löffler, D. Strash and L. Trott, "Category-Based Routing in Social Networks: Membership Dimension and the Small-World Phenomenon," *IEEE Int. Conf. on Computational Aspects of Social Networks* (CASoN), 102–107, 2011. (Preliminary version of J-84.)

C-165. M.T. Goodrich, O. Ohrimenko, M. Mitzenmacher, and R. Tamassia, "Privacy-Preserving Group Data Access via Stateless Oblivious RAM Simulation," *23rd ACM-SIAM Symp. on Discrete Algorithms* (SODA), 157–167, 2012.

C-166. M.T. Goodrich, O. Ohrimenko, M. Mitzenmacher, and R. Tamassia, "Practical Oblivious Storage," *2nd ACM Conf. on Data and Application Security and Privacy* (CODASPY). 13–24, 2012.

C-167. M.T. Goodrich and M. Mitzenmacher, "Anonymous Card Shuffling and its Applications to Parallel Mixnets," *39th Int. Colloquium on Automata, Languages and Programming* (ICALP), Springer, LNCS, vol. 6756, 576–587, 2012.

C-168. M.T. Goodrich, O. Ohrimenko, and R. Tamassia, "Graph Drawing in the Cloud: Privately Visualizing Relational Data using Small Working Storage," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 43–54, 2012.

C-169. F.J. Brandenburg, D. Eppstein, A. Gleissner, M.T. Goodrich, K. Hanauer, and J. Reislhuber, "On the Density of Maximal 1-Planar Graphs," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 327–338, 2012.

C-170. M.J. Bannister, D. Eppstein, M.T. Goodrich, and L. Trott, "Force-Directed Graph Drawing Using Social Gravity and Scaling," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 414–425, 2012.

C-171. M.T. Goodrich and J.A. Simons, "More Graph Drawing in the Cloud: Data-Oblivious st-Numbering, Visibility Representations, and Orthogonal Drawing of Biconnected Planar Graphs," *20th Int. Symp. on Graph Drawing* (GD), Springer, LNCS, vol. 7704, 569–570, 2012.

C-172. M.T. Goodrich, D.S. Hirschberg, M. Mitzenmacher, and J. Thaler, "Cache-Oblivious Dictionaries and Multimaps with Negligible Failure Probability," *Mediterranean Conf. on Algorithms* (MedAlg), Springer, LNCS, vol. 7659, 203–218, 2012.

C-173. D. Eppstein, M.T. Goodrich, and D.S. Hirschberg, "Combinatorial Pair Testing: Distinguishing Workers from Slackers," *Algorithms and Data Structures Symp.* (WADS), Springer, LNCS, vol. 8037, 316–327, 2013.

C-174. D. Eppstein, M.T. Goodrich, and J.A. Simons, "Set-Difference Range Queries," *25th Canadian Conf. on Computational Geometry* (CCCG), 2013, http://www.cccg.ca/proceedings/2013/.

C-175. M.T. Goodrich and P. Pszona, "Cole's Parametric Search Technique Made Practical," *25th Canadian Conf. on Computational Geometry* (CCCG), 2013,

http://www.cccg.ca/proceedings/2013/.

C-176. L. Arge, M.T. Goodrich, F. van Walderveen, "Computing Betweenness Centrality in External Memory," *IEEE Int. Conf. on Big Data* (BigData), 368–375, 2013.

C-177. M.T. Goodrich and P. Pszona, "Achieving Good Angular Resolution in 3D Arc Diagrams," *21st Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8242, 161–172, 2013.

C-178. M.T. Goodrich and P. Pszona, "Streamed Graph Drawing and the File Maintenance Problem," *21st Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8242, 256–267, 2013.

C-179. M.T. Goodrich, "Zig-zag Sort: A Simple Deterministic Data-Oblivious Sorting Algorithm Running in $O(n \log n)$ Time," *46th ACM Symp. on Theory of Computing* (STOC), 684–693, 2014.

C-180. D. Eppstein, M.T. Goodrich, M. Mitzenmacher, and P. Pszona, "Wear Minimization for Cuckoo Hashing: How Not to Throw a Lot of Eggs into One Basket," *Symp. on Experimental Algorithms* (SEA), Springer, LNCS, vol. 8504, 162–173, 2014.

C-181. O. Ohrimenko, M.T. Goodrich, and R. Tamassia, an E. Upfal, "The Melbourne Shuffle: Improving Oblivious Storage in the Cloud," *41st Int. Colloq. on Automata, Languages, and Programming* (ICALP), Springer, LNCS, vol. 8573, 556–567, 2014.

C-182. M.J. Bannister, W.E. Devanny, M.T. Goodrich, J.A. Simons, and Lowell Trott, "Windows into Geometric Events: Data Structures for Time-Windowed Querying of Temporal Point Sets," *26th Canadian Conf. on Computational Geometry* (CCCG), 2014.

C-183. M.J. Bannister, W.E. Devanny, D. Eppstein and M.T. Goodrich, "The Galois Complexity of Graph Drawing: Why Numerical Solutions are Ubiquitous for Force-Directed, Spectral, and Circle Packing Drawings," *22nd Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8871, 149–161, 2014. (Preliminary version of J-86.)

C-184. M.J. Alam, D. Eppstein, M.T. Goodrich, S. Kobourov and S. Pupyrev, "Balanced Circle Packings for Planar Graphs," *22nd Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8871, 125–136, 2014.

C-185. M. Bannister, M.T. Goodrich, and P. Sampson, "Force-Directed 3D Arc Diagrams," *22nd Int. Symp. Graph Drawing* (GD), Springer, LNCS, vol. 8871, 521–522, 2014.

C-186. M.T. Goodrich and P. Pszona, "Two-Phase Bicriterion Search for Finding Fast and Efficient Electric Vehicle Routes," *22nd ACM SIGSPATIAL Int. Conf. on Adv. Geographic Information Systems* (GIS), 193–202, 2014.

C-187. M.T. Goodrich and J. Simons, "Data-Oblivious Graph Algorithms in Outsourced External Memory," *8th Int. Conf. on Combinatorial Optimization and Applications* (COCOA), LNCS, Vol. 8881, 241–257, 2014.

C-188. M.T. Goodrich, T. Johnson, M. Torres, "Knuthian Drawings of Series-Parallel Flowcharts," *23rd Int. Symp. on Graph Drawing and Network Visualization* (GD), Springer, LNCS, vol. 9411, 556–557, 2015. (See also http://arxiv.org/abs/1508.03931.)

C-189. M.T. Goodrich and A. Eldawy, "Parallel Algorithms for Summing Floating-Point Numbers," *28th ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 13–22, 2016.

C-190. W.E. Devanny, M.T. Goodrich, and K. Jetviroj, "Parallel Equivalence Class Sorting: Algorithms, Lower Bounds, and Distribution-Based Analysis," *28th ACM Symp. on Parallel Algorithms and Architectures* (SPAA), 265–274, 2016.

C-191. D. Eppstein, M.T. Goodrich, J. Lam, N. Mamano, M. Mitzenmacher, and M. Torres, "Models and Algorithms for Graph Watermarking," *19th Information Security Conf.* (ISC), 283–301, 2016. **Best Student Paper Award**.

C-192. E. Ghosh, M.T. Goodrich, O. Ohrimenko, R. Tamassia, "Verifiable Zero-Knowledge Order

Queries and Updates for Fully Dynamic Lists and Trees," *10th Conf. on Security and Cryptography for Networks* (SCN), 216–236, 2016.

C-193. M.T. Goodrich, E. Kornaropoulos, M. Mitzenmacher, R. Tamassia, "More Practical and Secure History-Independent Hash Tables," *21st European Symp. on Research in Computer Security* (ESORICS), 20-38, 2016.

C-194. J.J. Besa Vial, W.E. Devanny, D. Eppstein, and M.T. Goodrich, "Scheduling Autonomous Vehicle Platoons Through an Unregulated Intersection," *2016 Workshop on Algorithmic Approaches for Transportation Modeling, Optimization, and Systems* (ATMOS), 5:1–5:14.

C-195. M.J. Alam, M.B. Dillencourt, and M.T. Goodrich, "Capturing Lombardi Flow in Orthogonal Drawings by Minimizing the Number of Segments," *24th Int. Symp. on Graph Drawing and Network Visualization* (GD), LNCS, Vol. 9801, 608–610, 2016.

C-196. M.J. Alam, M.T. Goodrich, and T. Johnson, "Sibling-First Recursive Graph Drawing for Java Bytecode," *24th Int. Symp. on Graph Drawing and Network Visualization* (GD), LNCS, Vol. 9801, 611–612, 2016.

C-197. M.T. Goodrich, S. Gupta, and M. Torres, "A Topological Algorithm for Determining How Road Networks Evolve Over Time," *24th ACM SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems* (GIS), 31:1–31:10, 2016.

C-198. M.J. Alam, M.T. Goodrich, and T. Johnson, "J-Viz: Finding Algorithmic Complexity Attacks via Graph Visualization of Java Bytecode," *13th IEEE Symp. on Visualization for Cyber Security* (VizSec), 1–8, 2016.

C-199. M.T. Goodrich, E. Kornaropoulos, M. Mitzenmacher, and R. Tamassia, "Auditable Data Structures," *2nd IEEE European Symp. on Security and Privacy* (EuroS&P), 285–300, 2017.

C-200. D. Eppstein, M.T. Goodrich, M. Mitzenmacher, and M. Torres, "2-3 Cuckoo Filters for Faster Triangle Listing and Set Intersection," 36th ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems (PODS), 247–260, 2017.

C-201. D. Eppstein, M.T. Goodrich, and N. Mamano, "Algorithms for Stable Matching and Clustering in a Grid," 18th International Workshop on Combinatorial Image Analysis (IWCIA), 117–131, 2017.

C-202. G. Ateniese, M.T. Goodrich, V. Lekakis, C. Papamanthou, E. Paraskevas, and R. Tamassia, "Accountable Storage," 15th International Conference on Applied Cryptography and Network Security (ACNS), 623–644, 2017.

C-203. D. Eppstein and M.T. Goodrich, "Brief Announcement: Using Multi-Level Parallelism and 2-3 Cuckoo Filters for Faster Set Intersection Queries and Sparse Boolean Matrix Multiplication," 29th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 137–139, 2017.

C-204. W.E. Devanny, J. Fineman, M.T. Goodrich, and T. Kopelowitz, "The Online House Numbering Problem: Min-Max Online List Labeling," 25th European Symposium on Algorithms (ESA), 33:1–33:15, 2017.

C-205. M.T. Goodrich, "Answering Spatial Multiple-Set Intersection Queries Using 2-3 Cuckoo Hash-Filters," 25th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS), 65:1–65:4, 2017.

C-206. D. Eppstein, M.T. Goodrich, D. Korkmaz, and N. Maman, "Defining Equitable Geographic Districts in Road Networks via Stable Matching," 25th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS), 52:1–52:4, 2017.

C-207. M.T. Goodrich, "BIOS ORAM: Improved Privacy-Preserving Data Access for Parameterized Outsourced Storage,' ACM Workshop on Privacy in the Electronic Society (WPES),

held in conjunction with the ACM Conf. on Computer and Communications Security (CCS), 41–50, 2017.

C-208. J.J. Besa Vial, W.E. Devanny, D. Eppstein, M.T. Goodrich, and T. Johnson, "Quadratic Time Algorithms Appear to be Optimal for Sorting Evolving Data," Algorithm Engineering & Experiments (ALENEX), 87–96, 2018.

C-209. D. Eppstein, M.T. Goodrich, N. Mamano, "Reactive Proximity Data Structures for Graphs," 13th Latin American Theoretical Informatics Symposium (LATIN), LNCS, Vol. 10807, Springer, 777–789, 2018.

C-210. M.T. Goodrich, "Isogrammic-Fusion ORAM: Improved Statistically Secure Privacy-Preserving Cloud Data Access for Thin Clients," 13th ACM ASIA Conf. on Information, Computer and Communications Security (ASIACCS), 699–706, 2018.

C-211. J.J. Besa Vial, W.E. Devanny, D. Eppstein, M.T. Goodrich, and T. Johnson, "Optimally Sorting Evolving Data," 45th Int. Colloq. on Automata, Languages, and Programming (ICALP), 81:1–81:13, 2018.

C-212. G. Barequet, D. Eppstein, M.T. Goodrich, and N. Mamano, "Stable-Matching Voronoi Diagrams: Combinatorial Complexity and Algorithms," 45th Int. Colloq. on Automata, Languages, and Programming (ICALP), 89:1–89:14, 2018.

C-213. G. Da Lozzo, D. Eppstein, M.T. Goodrich, and S. Gupta, "Subexponential-Time and FPT Algorithms for Embedded Flat Clustered Planarity," 44th Int. Workshop on Graph-Theoretic Concepts in Computer Science (WG), 111–124, 2018.

C-214. G. Barequet, M. De, and M.T. Goodrich, "Computing Convex-Straight-Skeleton Voronoi Diagrams for Segments and Convex Polygons," The 24th International Computing and Combinatorics Conference (COCOON), 130–142, 2018.

C-215. M.T. Goodrich and T. Johnson, "Low Ply Drawings of Trees and 2-Trees," 30th Canadian Conference on Computational Geometry (CCCG), 1–9, 2018.

C-216. D. Eppstein, M.T. Goodrich, J. Jorgensen, and M.R. Torres, "Geometric Fingerprint Recognition via Oriented Point-Set Pattern Matching," 30th Canadian Conference on Computational Geometry (CCCG), 1–16, 2018.

Other Publications:

O-1. M.T. Goodrich, "Guest Editor's Introduction," *International Journal of Computational Geometry & Applications*, **2**(2), 1992, 113–116.

O-2. M.T. Goodrich, "Parallel Algorithms Column 1: Models of Computation," *SIGACT News*, **24**(4), 1993, 16–21.

O-3. M.T. Goodrich, V. Mirelli, M. Orletsky, and J. Salowe, "Decision tree construction in fixed dimensions: Being global is hard but local greed is good," Technical Report TR-95-1, Johns Hopkins University, Department of Computer Science, Baltimore, MD 21218, May 1995.

O-4. R. Tamassia, P.K. Agarwal, N. Amato, D.Z. Chen, D. Dobkin, R.L.S. Drysdale, S. Fortune, M.T. Goodrich, J. Hershberger, J. O'Rourke, F.P. Preparata, J.-R. Sack, S. Suri, I.G. Tollis, J.S. Vitter, and S. Whitesides, "Strategic Directions in Computational Geometry Working Group Report," *ACM Computing Surveys*, **28A**(4), December 1996.

O-5. G.A. Gibson, J.S. Vitter, and J. Wilkes, A. Choudhary, P. Corbett, T.H. Cormen, C.S. Ellis, M.T. Goodrich, P. Highnam, D. Kotz, K. Li, R. Muntz, J. Pasquale, M. Satyanarayanan, D.E. Vengroff, "Report of the Working Group on Storage I/O Issues in Large-Scale Computing," *ACM Computing Surveys*, **28A**(4), December 1996.

O-6. T.H. Cormen and M.T. Goodrich, "A Bridging Model for Parallel Computation, Communication, and I/O," *ACM Computing Surveys*, **28A**(4), December 1996.

O-7. M.T. Goodrich, "Computer Science Issues in the National Virtual Observatory," in *Virtual Observatories of the Future*, ASP Conf. Series, vol. 225, R.J. Brunner, S.G. Djorgovski, and A.S. Szalay, eds., 329–332, 2001.

O-8. M.T. Dickerson and M.T. Goodrich, "Matching Points to a Convex Polygonal Boundary," Proceedings of the 13th Canadian Conf. on Computational Geometry (CCCG'01), 89–92, 2001.

O-9. M.T. Goodrich, "Guest Editor's Foreword," *Algorithmica*, **33**(3), 271, 2002.

O-10. M.T. Goodrich, M. Shin, C.D. Straub, and R. Tamassia, "Distributed Data Authentication (System Demonstration)," *DARPA Information Survivability Conf. and Exposition*, IEEE Press, Volume 2, 58–59, 2003.

O-11. M.T. Goodrich and R. Tamassia, "Efficient and Scalable Infrastructure Support for Dynamic Coalitions," *DARPA Information Survivability Conf. and Exposition*, IEEE Press, Volume 2, 246–251, 2003.

O-12. E. Ghosh, M.T. Goodrich, O. Ohrimenko, and R. Tamassia, "Poster: Zero-Knowledge Authenticated Order Queries and Applications," *IEEE Symp. on Security and Privacy*, 2015. (See also https://eprint.iacr.org/2015/283.)

O-13. F. Bayatbabolghani, M. Blanton, M. Aliasgari, and M.T. Goodrich, "Poster: Secure Computations of Trigonometric and Inverse Trigonometric Functions," *IEEE Symposium on Security and Privacy*, 2017.

PROFESSIONAL SERVICE

Guest Editor:

Int. Journal of Computational Geometry & Applications, **2**(2), 1992
Journal of Computer & System Sciences, **52**(1), 1996
Computational Geometry: Theory and Applications, **12(1–2)**, 1999.
Algorithmica, **33**(3), 2002.

Editorial Board Membership:

Computational Geometry: Theory and Applications, 2006–2015
Journal of Computer & System Sciences, 1994–2011
Journal of Graph Algorithms and Applications, 1996–2011
Int. Journal of Computational Geometry & Applications, 1993–2010
Information Processing Letters, 1995–1997

Journal Advisory Board Membership:

Int. Journal of Computational Geometry & Applications, 2010–
Journal of Graph Algorithms and Applications, 2011–

Program Committee Service:

7th ACM Symp. on Computational Geometry (SoCG), 1991
1991 Workshop on Algorithms and Data Structures (WADS)
8th ACM Symp. on Computational Geometry (SoCG), 1992
25th ACM Symp. on Theory of Computing (STOC), 1993
Chair, 26th ACM Symp. on Theory of Computing (STOC), 1994
11th ACM Symp. on Computational Geometry (SoCG), 1995
DAGS '95 Conf. on Electronic Publishing and the Information Superhighway
1996 SIAM Discrete Mathematics Conference
1997 Workshop on Algorithms and Data Structures (WADS)
International Symposium on Graph Drawing (GD), 1997

1999 Workshop on Algorithms and Data Structures (WADS)
Co-chair, Workshop on Algorithm Engineering and Experimentation (ALENEX), 1999
International Symposium on Graph Drawing (GD), 2000
2000 Workshop on Algorithm Engineering (WAE)
41st IEEE Symp. on Foundations of Computer Science (FOCS), 2000
2001 Workshop on Algorithms and Data Structures (WADS)
International Symposium on Graph Drawing (GD), 2001
Workshop on Algorithm Engineering and Experimentation (ALENEX), 2002
18th ACM Symp. on Computational Geometry (SoCG), 2002
13th ACM-SIAM Symp. on Discrete Algorithms (SODA), 2002
Co-Chair, Graph Drawing 2002
International Symposium on Graph Drawing (GD), 2003
16th ACM-SIAM Symp. on Discrete Algorithms (SODA), 2005
32nd Int. Colloq. on Automata, Languages and Programming (ICALP), 2005
12th Int. Computing and Combinatorics Conference (COCOON), 2006
13th ACM Conf. on Computer and Communication Security (CCS), 2006
15th Annual European Symposium on Algorithms (ESA), 2007
5th International Conference on Applied Cryptography and Network Security (ACNS), 2007
21st IEEE International Parallel & Distributed Processing Symposium (IPDPS), 2007
19th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 2007
5th Workshop on Algorithms and Models for the Web-Graph (WAW), 2007
7th International Workshop on Experimental Algorithms (WEA), 2008
Second International Frontiers of Algorithmics Workshop (FAW), 2008
16th ACM SIGSPATIAL Int. Symp. on Adv. in Geographic Information Systems (GIS), 2008
17th ACM SIGSPATIAL Int. Symp. on Adv. in Geographic Information Systems (GIS), 2009
31st IEEE Symposium on Security and Privacy (SSP), 2010
18th Int. Symp. on Graph Drawing (GD), 2010
2011 Workshop on Analytic Algorithmics and Combinatorics (ANALCO)
8th Workshop on Algorithms and Models for the Web Graph (WAW), 2011
19th International Symposium on Graph Drawing (GD), 2011
24th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 2012
20th European Symposium on Algorithms (ESA), 2012
2013 IEEE Int. Conf. on Big Data (BigData), 2013
30th IEEE Int. Conf. on Data Engineering (ICDE), 2014
21st ACM Conf. on Computer and Communication Security (CCS), 2014
Sympoisum on Algorithms and Data Structures (WADS), 2015
ACM Cloud Computing Security Workshop (CCSW), 2015
International Symposium on Graph Drawing (GD), 2015
co-chair, 2016 Workshop on Algorithm Engineering and Experiments (ALENEX)
2016 Workshop on Massive Data Algorithmics (MASSIVE)
2016 Int. Symposium on Algorithms and Computation (ISAAC)
29th ACM Symposium on Parallelism in Algorithms and Architectures (SPAA), 2017
25th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems (GIS), 2017
26th European Symposium on Algorithms (ESA), 2018
26th ACM SIGSPATIAL Int. Conf. on Adv. in Geographic Information Systems (GIS), 2018
2nd Symposium on Simplicity in Algorithms (SOSA), 2019
1st ACM SIGSPATIAL Int. Workshop on Spatial Gems, 2019

Conference/Workshop Committee Service:

Conference chair, 12th ACM Symposium on Computational Geometry, 1996
Organizer, 1st CGC Workshop on Computational Geometry, 1996
Co-chair, 1999 Dagstuhl Workshop on Computational Geometry, 1999

Conference chair, Graph Drawing, 2002

Co-organizer, Hawaiian Workshop on Parallel Algorithms, 2017

Steering Committee and Executive Committee Service:

Member at large, ACM SIG on Algorithms & Comp. Theory (SIGACT) Exec. Comm., 1993–97

Member, Exec. comm. for 1996 Federated Computing Research Conference (FCRC)

co-Founder and member, Steering Comm. for Workshop on Algorithm Engineering and Experimentation (ALENEX), 1999– (chair, 2014–16)

co-Chair, Steering Comm. for ACM Symposium on Computational Geometry, 1999–2001

Member, Steering Comm. for Graph Drawing Conference, 2000–2003, 2014–

Conference Chair, ACM SIG on Algorithms & Comp. Theory (SIGACT), 2005–2009

Review Panelist:

National Science Foundation, 2000–2017

Ph.D. Advisees:

Mujtaba Ghouse	"Randomized Parallel Computational Geometry in Theory and Practice," May 1993.
Paul Tanenbaum	"On Geometric Representations of Partially Ordered Sets," May 1995 (co-advised with Prof. Edward Scheinerman).
Mark Orletsky	"Practical Methods for Geometric Searching Problems with Experimental Validation," May 1996.
Kumar Ramaiyer	"Geometric Data Structures and Applications," Aug. 1996.
Christian Duncan	"Balanced Aspect Ratio Trees," Aug. 1999.
Christopher Wagner	"Graph Visualization and Network Routing," Oct. 1999 (co-advised with Prof. Lenore Cowen)
Stephen Kobourov	"Algorithms for Drawing Large Graphs," May 2000
Amitabha Bagchi	"Efficient Strategies for Topics in Internet Algorithmics," Oct. 2002
Amitabh Chaudhary	"Applied Spatial Data Structures for Large Data Sets," Oct. 2002
Jeremy Yu Meng	"Confluent Graph Drawing," June 2006
Jonathan Zheng Sun	"Algorithms for Hierarchical Structures, with Applications to Security and Geometry," August 2006
Nodari Sitchinava	"Parallel External Memory Model—A Parallel Model for Multi-core Architectures," Sept. 2009
Darren Strash	"Algorithms for Sparse Geometric Graphs and Social Networks," May 2011 (co-advised with with David Eppstein)
Lowell Trott	"Geometric Algorithms for Social Network Analysis," May 2013
Joseph Simons	"New Dynamics in Geometric Data Structures," May 2014
Pawel Pszona	"Practical Algorithms for Sparse Graphs," May 2014
William E. Devanny	"An Assortment of Sorts: Three Modern Variations on the Classic Sorting Problem," July 2017 (co-advised with with David Eppstein)
Siddharth Gupta	"Topological Algorithms for Geographic and Geometric Graphs," August 2018 (co-advised with with David Eppstein)
Timothy Johnson	"Graph Drawing Representations and Metrics with Applications," August 2018

Ph.D. Committee Service:

John Augustine	UC-Irvine	Advancement to candidacy, September 2003
Nikos Triandopoulos	Brown U.	Thesis prelim., February 2004
Einar Mykletun	UC-Irvine	Advancement to candidacy, March 2004
Kartic Subr	UC-Irvine	Advancement to candidacy, September 2004
S. Joshua Swamidass	UC-Irvine	Advancement to candidacy, April 2005

Jeong Hyun Yi	UC-Irvine	Thesis defense, August, 2005
Nodari Sitchinava	UC-Irvine	Advancement to candidacy, chair, December 2005
John Augustine	UC-Irvine	Thesis defense, July 2006
Maithili Narasimha	UC-Irvine	Thesis defense, August, 2006
Josiah Carlson	UC-Irvine	Advancement to candidacy, August 2006
Xiaomin Liu	UC-Irvine	Advancement to candidacy, September 2006
Gabor Madl	UC-Irvine	Advancement to candidacy, September 2006
Nikos Triandopoulos	Brown U.	Thesis defense, September 2006
Rabia Nuray-Turan	UC-Irvine	Advancement to candidacy, May 2007
S. Joshua Swamidass	UC-Irvine	Thesis defense, June 2007
Michael Sirivianos	UC-Irvine	Advancement to candidacy, June 2007
Kevin Wortman	UC-Irvine	Advancement to candidacy, August 2007
Di Ma	UC-Irvine	Advancement to candidacy, December 2007
Josiah Carlson	UC-Irvine	Thesis defense, December 2007
Michael Nelson	UC-Irvine	Advancement to candidacy, chair, March 2008
Minas Gjoka	UC-Irvine	Advancement to candidacy, June 2008
Sara Javanmardi	UC-Irvine	Advancement to candidacy, June 2008
Ali Zandi	UC-Irvine	Advancement to candidacy, September 2008
Jihye Kim	UC-Irvine	Thesis defense, September 2008
Darren Strash	UC-Irvine	Advancement to candidacy, December 2008
Kevin Wortman	UC-Irvine	Topic defense, January 2009
Nodari Sitchinava	UC-Irvine	Topic defense, chair, June 2009
Fabio Soldo	UC-Irvine	Advancement to candidacy, July 2009
Emil De Cristofaro	UC-Irvine	Advancement to candidacy, July 2009
Di Ma	UC-Irvine	Thesis defense, August 2009
Yanbin Lu	UC-Irvine	Advancement to candidacy, December 2009
Anh Le	UC-Irvine	Advancement to candidacy, April 2010
Lowell Trott	UC-Irvine	Advancement to candidacy, June 2010
Xiaomin Liu	UC-Irvine	Thesis defense, August 2010
Josh Olsen	UC-Irvine	Advancement to candidacy, September 2010
Yasser Altowim	UC-Irvine	Advancement to candidacy, December 2010
Angela Wong	UC-Irvine	Advancement to candidacy, May 2011
Joshua Hill	UC-Irvine	Advancement to candidacy, September 2011
Alex Abatzoglou	UC-Irvine	Advancement to candidacy, September 2011
Michael Wolfe	UC-Irvine	Masters Thesis defense, October 2011
Olya Ohrimenko	Brown Univ.	PhD Thesis proposal, October 2011
Yanbin Lu	UC-Irvine	PhD Thesis defense, November 2011
Chun Meng	UC-Irvine	Advancement to candidacy, December 2011
Abinesh Ramakrishnan	UC-Irvine	Advancement to candidacy, March 2012
Pegah Sattari	UC-Irvine	PhD Thesis defense, April 2012
Michael Bannister	UC-Irvine	PhD Thesis defense, May 2015
Yingyi Bu	UC-Irvine	PhD Thesis defense, August 2015
Jenny Lam	UC-Irvine	PhD Thesis defense, November 2015
Timothy Johnson	UC-Irvine	Advancement to candidacy, chair, June 2016
Jiayu Xu	UC-Irvine	Advancement to candidacy, November 2016
Sky Faber	UC-Irvine	PhD Thesis defense, November 2016
Juan Jose Besa Vial	UC-Irvine	Advancement to candidacy, chair, March 2017
Ingo van Duijn	Aarhus Univ.	PhD Thesis defense, September 2017

Boyang Wei UC-Irvine PhD Thesis defense, August 2018

University Service:

Ph.D. Requirements Committee, Dept. of Computer Science, chair: 1987–89
Graduate Admissions Committee, Dept. of Computer Science, 1991–1993 (chair: 1992)
Faculty Recruiting Committee, Dept. of Computer Science, 1993,95,96 (chair: 1996)
Steering Committee, Whiting School of Engineering, 1990–93 (chair, 1993)
Johns Hopkins Homewood Academic Computing Oversight Committee, 1990–93
Curriculum Committee, Whiting School of Engineering, 1994–96
Strategic Planning Committee, Whiting School of Engineering, 1999–00
Graduate Policy Committee, UCI Dept. of Information & Computer Science (ICS), 2001–02
Faculty Search Committee in Cryptography, UCI Dept. of ICS, 2001–03
School of Info. and Computer Science Executive Committee, 2002–04
UCI Committee on Educational Policy (CEP), 2002–03, 2004–06
UCI Change of Major Criteria Committee, 2002–03
UCI CEP Policy Subcommittee, 2002–2003
Distinguished Faculty Search Committee, Bren School of ICS, 2004–11 (chair, 2007–08)
Equity Advisor, Bren School of ICS, 2005–09
Dean's Advisory Council, Bren School of ICS, 2007–13
Associate Dean for Faculty Development, Bren School of ICS, 2006–12
Chair, Department of Computer Science, Bren School of ICS, 2012–13
Master of Computer Science Development Committee, Bren School of ICS, 2013–2016
Stragic Planning Committee, Dept. of Computer Science, Bren School of ICS, 2015–16
Master of Computer Science Steering Committee, Bren School of ICS, 2016–
Executive Committee, Bren School of ICS, 2017–18
UC-Irvine Committee on Scholarly Honors & Awards, 2017–
UC-Irvine Special Research Program Review Committee for CalIT2, 2018–19

Courses Taught and Developed:

Advanced Parallel Computing (developed and taught at Hopkins)
Cyber-Puzzlers (designed and taught at UCI)
Computer Literacy (taught at Purdue, developed at Hopkins)
Computer Programming for Scientists and Engineers (taught at Purdue)
Computer Security Algorithms (developed and taught at UCI)
Computational Models (revised and taught at Hopkins)
Computational Geometry (revised and taught at Hopkins and UCI)
Compiler Theory and Design (revised and taught at Hopkins)
Computer Graphics (taught at Hopkins)
Cyber-Fraud Detection and Prevention (designed and taught at UCI)
Data Structures (revised and taught at Hopkins and UCI)
Graph Algorithms (revised and taught at UCI)
Formal Languages and Automata Theory (revised and taught at UCI)
Fundamentals of Algorithms with Applications (revised and taught at UCI)
Introduction to Algorithms (developed and taught at Hopkins and UCI)
Internet Algorithmics (developed and taught at Hopkins, Brown, and UCI)
Design and Analysis of Algorithms (revised and taught at Hopkins and UCI)
Parallel Algorithms (developed and taught at Hopkins and Univ. of Illinois)
Project in Algorithms and Data Structures (revised and taught at UCI)

Scientific Consulting:

APAC Security, Inc., 2005
Algomagic Technologies, Inc., 2000–2005
Army Research Laboratory, Fort Belvior, 1995
AT&T, 1998
Battelle Research Triangle, Columbus Division, 1996
Brown University, 2000–2007
3M, 2015
Purdue University, 2002
The National Science Foundation, 1990–2016
Univ. of Miami, 1999
Walt Disney Animation Studios, 2009

Technical Expert Consulting (last four years):

- 2014–15, Technical expert, deponent, and testifying witness, McKool Smith, PC (Dallas) and ContentGuard Holdings, in patent litigation.
- 2014–17, Technical expert, Kirkland & Ellis, LLP (Chicago) and IBM, in patent litigation.
- 2014–16, Technical expert and deponent, Fenwick & West, LLP (San Francisco) and Symantec, in patent litigation.
- 2016, Technical expert, deponent, and testifying witness, Dentons US LLP., in confidential arbitration.
- 2016, Technical expert, Sheppard Mullin Richter & Hampton LLP (Los Angeles), in non-patent intellectual property dispute.
- 2016–, Technical expert and deponent, Kramer Levin Naftalis & Frankel LLP (Menlo Park, CA) and Acceleration Bay LLC, in patent litigation.
- 2016–, Technical expert and deponent, Kramer Levin Naftalis & Frankel LLP (Menlo Park, CA) and Finjan, Inc., in patent litigation.
- 2017–, Technical expert, Fitzpatrick, Cella, Harper & Scinto, and Koninklijke Philips N.V., in patent litigation.
- 2017–18, Technical expert and deponent, Haynes and Boone, LLP, and mSIGNIA in patent litigation.
- 2017–19, Technical expert and deponent, Thompson & Knight LLP and SEVEN Networks LLC, in patent litigation.
- 2018–, Technical expert, deponent, and testifying witness, Kramer Levin Naftalis & Frankel LLP (Menlo Park, CA) and Centripetal Networks, in patent litigation.
- 2019–, Technical expert and deponent, McKool Smith and SEVEN Networks LLC, in patent litigation.
- 2019–, Technical expert, Kramer Levin Naftalis & Frankel LLP (Menlo Park, CA) and CUPP Cybersecurity LLC, et al., in patent litigation.

GRANTS AND CONTRACTS

1. PI, "Research Initiation Award: Parallel and Sequential Computational Geometry," National Science Foundation (NSF Grant CCR-8810568), $32,914, 1988–90.
2. co-PI, "Paradigms for Parallel Algorithm Design," NSF and DARPA (as NSF Grant CCR-8908092), $523,837, 1989–93 (with S.R. Kosaraju (PI), S. Kasif, and G. Sullivan).
3. PI, "Parallel Computation and Computational Geometry," NSF (Grant CCR-9003299), $67,436, 1990–93.
4. co-PI, "A Facility for Experimental Validation," NSF (Grant CDA-9015667), $1,476,147, 1991–96 (with G. Masson (PI), J. Johnstone, S. Kasif, S.R. Kosaraju, S. Salzberg, S. Smith,

G. Sullivan, L. Wolff, and A. Zwarico).

5. PI, "Parallel Network Algorithms for Cell Suppression," The Bureau of the Census (JSA 91-23), $14,998 1991–92.
6. PI, "A Geometric Framework for the Exploration & Analysis of Astrophysical Data," NSF (Grant IRI-9116843), $535,553, 1991–96 (with S. Salzberg and H. Ford (from Physics and Astronomy Dept.)).
7. PI, "Research Experiences for Undergraduates supplement to IRI-9116843," NSF, $4,000, 1993–94 (with S. Salzberg and H. Ford).
8. PI, "Constructing, Maintaining, and Searching Geometric Structures," NSF (Grant CCR-9300079), $134,976, 1993–96.
9. co-PI, "Robust and Applicable Geometric Computing," Army Research Office (ARO MURI Grant DAAH04-96-1-0013), $4,500,000, 1996–2000 (with F. Preparata (PI, Brown U.), R. Tamassia (Brown U.), S. Rao Kosaraju, J. Vitter (Duke U.), and P. Agarwal (Duke U.)). Subaward size: $1,466,640.
10. PI, "Application-Motivated Geometric Algorithm Design," NSF (Grant CCR-9625289), $107,389, 1996-98.
11. co-PI, "vBNS Connectivity for the Johns Hopkins University," NSF, $350,000, 1997–99 (with T.O. Poehler (PI), D.J. Binko, J.G. Neal, and A.S. Szalay).
12. co-PI, "Product Donation, Technology for Education Program," Intel Corporation, $480,071, 1997–2001 (with T.O. Poehler (PI), J.H. Anderson, A.S. Szalay, and M. Robbins).
13. co-PI, "A Networked Computing Environment for the Manipulation & Visualization of Geometric Data" (Research Infrastructure), NSF, $1,638,785, 1997–2003 (with L.B. Wolff (PI), Y. Amir, S.R. Kosaraju, S. Kumar, R. Tamassia (Brown U.), R.H. Taylor, and D. Yarowsky).
14. PI, "Geometric Algorithm Design and Implementation," NSF, Grant CCR-9732300, $224,982, 1998–2002.
15. PI, "Certification Management Infrastructure – Certificate Revocation," $52,023, 1998, NSA LUCITE grant.
16. PI, "Software Engineering Data Loading, Analysis, and Reporting," $41,614, 1998, NSA LUCITE grant.
17. PI, "Establishing a LUCITE Collaboration Environment," $10,018, 1998, NSA LUCITE grant.
18. PI, "In Support of a Secure Multilingual Collabortive Computing Environment," $51,471, 1999-2000, NSA LUCITE grant.
19. PI, "Accessing Large Distributed Archives in Astronomy and Particle Physics," $199,981. subcontract to UCI from Johns Hopkins Univ. on NSF Grant PHY-9980044 (total budget, $2,500,000), 1999–2004.
20. PI, "Efficient and Scalable Infrastructure Support for Dynamic Coalitions," $1,495,000, DARPA Grant F30602-00-2-0509, 2000-2003 (with Robert Cohen and Roberto Tamassia), including $227,893 subaward to UCI (with Gene Tsudik).
21. PI, "Graph Visualization and Geometric Algorithm Design," $400,000, NSF Grant CCR-0098068, 2001-2004 (with Roberto Tamssia).
22. PI, "Collaborative Research: Teaching Data Structures to the Millennium Generation," $125,00, NSF Grant DUE-0231467, 2003–2005.
23. PI, "Collaborative Research: An Algorithmic Approach to Cyber-Security," $100,000, NSF Grant CCR-0311720, 2003–2006.
24. PI, "The OptIPuter," $900,000, subcontract from UCSD on NSF ITR grant CCR-0225642 (total budget, $13.5 million), 2002–2007 (with Padhraic Smyth and Kane Kim).

25. PI, "ITR: Algorithms for the Technology of Trust," $300,000, NSF Grant CCR-0312760, 2003–2009.
26. co-PI, "SDCI Data New: Trust Management for Open Collaborative Information Repositories: The CalSWIM Cyberinfrastructure," NSF grant OCI-0724806, $1,103,590, 2007–2012.
27. co-PI, "Support for Machine Learning Techniques for Cyber-Fraud Detection," Experian Corporation, $200,000 gift, 2008.
28. PI, "IPS: Collaborative Research: Privacy Management, Measurement, and Visualization in Distributed Environments," NSF Grant IIS-0713046, $224,851, 2007–2009.
29. PI, "Collaborative Research: Algorithms for Graphs on Surfaces," $400,000, NSF Grant CCR-0830403, 2008–2011.
30. PI, "ROA Supplement: IPS: Collaborative Research: Privacy Management, Measurement, and Visualization in Distributed Environments," NSF Grant IIS-0847968, $25,000, 2008–2009.
31. co-investigator, "Scalable Methods for the Analysis of Network-Based Data," Office of Naval Research: Multidisciplinary University Research Initiative (MURI) Award, number N00014-08-1-1015, $529,152, 2008–2014.
32. PI, "EAGER: Usable Location Privacy for Mobile Devices," NSF Grant 0953071, $300,000, 2009–2011.
33. PI, "TC:Large:Collaborative Research: Towards Trustworthy Interactions in the Cloud," NSF Grant 1011840, $500,000, 2010-2015.
34. PI, "TWC: Medium: Collaborative: Privacy-Preserving Distributed Storage and Computation," NSF Grant 1228639, $390,738, 2012-2018.
35. PI, "Support for Research on Geometric Motion Planning," 3M Corporation, $40,000 gift, 2014.
36. PI, "A4V: Automated Analysis of Algorithm Attack Vulnerabilities," subcontract 10036982-UCI from University of Utah for DARPA agreement no. AFRL FA8750-15-2-0092, $980,000, 2015–2019.
37. PI, "TWC: Small: Collaborative: Practical Security Protocols via Advanced Data Structures," NSF Grant 1526631, $166,638, 2015–2018.
38. PI, "NSF-BSF: AF: Small: Geometric Realizations and Evolving Data," NSF Grant 1815073, $474,392, 2018–2021.

SELECTED INVITED TALKS (RECENT YEARS ONLY)

- "Probabilistic Packet Marking for Large-Scale IP Traceback," Purdue Univ., 2003
- "Algorithms for Data Authentication," Harvey Mudd College, 2003
- "Efficient Tree-Based Revocation in Groups of Low-State Devices," Univ. of Arizona, 2004
- "Leap-Frog Packet Linking and Diverse Key Distributions for Improved Integrity in Network Broadcasts," Southern California Security and Cryptography Workshop, 2005
- "Is Your Business Privacy Protected?," NEXT Connections, 2005
- "Distributed Peer-to-peer Data Structures," Harvard Univ., 2006
- "Balancing Life with an Academic Research Career," Grace Hopper Conference, 2006
- "Computer Security in the Large," Univ. Texas, San Antonio, 2006
- "Inspirations in Parallelism and Computational Geometry," Brown Univ., 2006
- "Efficiency and Security Issues for Distributed Data Structures," Computer Science Distinguished Lecture Series, Johns Hopkins Univ., 2006
- "Efficiency and Security Issues for Distributed Data Structures," UCLA, 2006

- "Efficiency and Security Issues for Distributed Data Structures," Edison Distinguished Lecturer Series, Univ. of Notre Dame, 2006
- "Efficiency and Security Issues for Distributed Data Structures," Computer Science Distinguished Lecturer Series, Texas A & M Univ., 2006
- "Algorithms for Secure Computing and Searching with Applications to Medical Informatics," Purdue Univ., 2006
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be Used for DNA Sequencing, Wireless Broadcasting, and Network Security," Univ. of Southern California, 2007
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be Used for DNA Sequencing, Wireless Broadcasting, and Network Security," Univ. California, San Diego, 2007
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be Used for DNA Sequencing, Wireless Broadcasting, and Network Security," Univ. Minnesota, 2007
- "Blood on the Database: How Algorithms for Testing Blood Samples can be Used for Database Integrity," Invited Keynote, 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec), 2007
- "Space-Efficient Straggler Identification," ALCOM Seminar, Univ. of Aarhus, 2007
- "Blood on the Computer: How Algorithms for Testing Blood Samples can be used in Modern Applications," ALCOM Seminar, Univ. of Aarhus, 2007
- "Studying Road Networks Through an Algorithmic Lens," ALCOM Seminar, Univ. of Aarhus, 2008
- "Studying Geometric Graph Properties of Road Networks Through an Algorithmic Lens," International Workshop on Computing: from Theory to Practice, 2009
- "Randomized Shellsort: A Simple Oblivious Sorting Algorithm," Distinguished Lecture Series, Department of Computer Science, Brown University, 2009
- "Simulating Parallel Algorithms in the MapReduce Framework with Applications to Parallel Computational Geometry," MASSIVE 2010
- "Data Cloning Attacks for Nearest-Neighbor Searching based on Retroactive Data Structures," Department of Computer Science, UCSB, 2011
- "Turning Privacy Leaks into Floods: Surreptitious Discovery of Social Network Friendships and Other Sensitve Binary Attribute Vectors," Department of Computer Science Distinguished Lecturer Series, Univ. of Illinois, Chicago, 2011
- "Turning Privacy Leaks into Floods: Surreptitious Discovery of Social Network Friendships and Other Sensitve Binary Attribute Vectors," Department of Computer Sciences, Purdue Univ., 2011
- "Spin-the-bottle Sort and Annealing Sort: Oblivious Sorting via Round-robin Random Comparisons," Department of Computer Science, Brown Univ., 2012
- "Using Data-Oblivious Algorithms for Private Cloud Storage Access," Qatar University, 2013
- "Using Data-Oblivious Algorithms for Private Cloud Storage Access," Department of Computer Science and Engineering Distinguished Speaker Series, University of Buffalo, 2013
- "Force-Directed Graph Drawing Using Social Gravity and Scaling," invited talk, ICERM Workshop on Stochastic Graph Models, Providence, RI, 2014
- "Invertible Bloom Lookup Tables and Their Applications in Large-Scale Data Analysis," invited key-note speaker, Algorithms for Big Data, Frankfurt, Germany, 2014
- "Invertible Bloom Lookup Tables and Their Applications in Large-Scale Data Analysis," Brown University, Providence, RI, 2014

- "Studying Road Networks Through an Algorithmic Lens," Bold Aspirations Visitor and Lecture, University of Kansas, 2015
- "Learning Character Strings via Mastermind Queries, with Case Studies," Invited Lecture, Workshop on Pattern Matching, Data Structures and Compression, Bar-Ilan University, Tel Aviv, Israel, 2016
- "Invertible Bloom Lookup Tables and Their Applications in Data Analysis," University of Hawaii, 2016
- "Invertible Bloom Lookup Tables," Purdue University, 2016
- "Combinatorial Pair Testing: Distinguishing Workers from Slackers," Calvin College, 2016
- "Invertible Bloom Lookup Tables," University of California, Riverside, 2016
- "2-3 Cuckoo Filters for Faster Triangle Listing and Set Intersection," Technion, Israel Institute of Technology, Haifa, Israel, 2017
- "2-3 Cuckoo Filters for Faster Triangle Listing and Set Intersection," University of Arizona, 2017
- "Parallel Computational Geometry," Hawaii Workshop on Parallel Algorithms and Data Structures, University of Hawaii, 2017

PROFESSIONAL SOCIETY MEMBERSHIPS

American Association for the Advancement of Science (AAAS), Fellow
IEEE and IEEE Computer Society, Fellow
Association for Computing Machinery (ACM), Fellow

TECHNICAL EXPERT CONSULTING SUMMARY
(LAST FOUR YEARS)

Michael T. Goodrich, PhD

Dept. of Computer Science
Bren School of Info. & Computer Sciences
University of California, Irvine
Irvine, CA 92697-3435

Phone: (949)824-9366
http://www.ics.uci.edu/~goodrich/
E-mail: goodrich (at) acm.org

TECHNICAL EXPERT CONSULTING

The following is a listing of prior and current expert consulting work for Michael T. Goodrich, PhD, for the last four years, but it may not include confidential information or confidential retentions, as per written agreements.

1. Mar. 2014 to Nov. 2015, Technical expert, deponent, and testifying expert at two trials, for McKool Smith, PC (Dallas) and ContentGuard Holdings, in patent litigation, ContentGuard Holdings v. Amazon, Apple, HTC, Samsung, Huawei, BlackBerry, and Motorola (Google). Civil Actions No. 2:13-cv-01112-JRG and 2:14-cv-00061-JRG (E.D. Tex.).

2. Apr. 2014 to Aug. 2017, Technical expert and deponent, for Kirkland & Ellis, LLP (Chicago), and IBM, through IMS Expert Services, in patent litigation, PersonalWeb and Level 3 Communications, LLC v. IBM. Civil Action No. 6:12-cv-00661 (E.D. Tex.).

3. Oct. 2014 to Feb. 2016, Technical expert and deponent, for Fenwick & West, LLP (San Francisco) and Symantec, through DOAR Expert Services, in several IPRs for patent litigation, Columbia University v. Symantec. IPR2015-00370, IPR2015-00371, and IPR2015-00372 (PTAB).

4. Feb. 2016 to May 2016, Technical expert, deponent, and testifying witness in non-patent arbitration hearing, for Dentons US LLP in confidential arbitration.

5. Apr. 2016 to present, Technical expert and deponent, for Kramer Levin LLP and Acceleration Bay LLC, in IPR proceedings and patent litigation, Acceleration Bay LLC v. Activision Bizzard, Inc., Electronic Arts Inc., Take-Two Interactive Software, Inc., Rockstar Games, Inc., and 2K Sports, Inc. Civil Actions No. 1:16-cv-00453-RGA, No. 1:16-cv-00454-RGA, No. 1:16-cv-00455-RGA (D. Del.), IPR2015-01951, IPR2015-01953, IPR2015-01964, IPR2015-01970, IPR2015-01972, IPR2015-01996, IPR2016-00724, and IPR2016-00747 (PTAB).

6. May 2016 to present, Technical expert and deponent, for Kramer Levin LLP and Finjan, Inc., in PTO proceedings and patent litigation, Finjan, Inc. v. Blue Coat, Finjan, Inc. v. ESET, LLC, Finjan, Inc. v. Juniper Networks, Inc., and Finjan, Inc. v. Cisco Systems, Inc. IPR2016-00478 (PTAB), and Civil Actions No. 5:13-cv-03999-BLF, 5:15-cv-03295-BLF-PSG (N.D. Cal.), 3:17-cv-05659-WHA (N.D. Cal.), and 17-cv-0072-BLF-SVK (N.D. Cal.).

7. Jun. 2016 to Oct. 2016, Technical expert, for Sheppard Mullin Richter & Hampton LLP in confidential non-patent intellectual property dispute.

8. Jan. 2017 to present, Technical expert, for Fitzpatrick, Cella, Harper & Scinto, Venable LLP, and Koninklijke Philips N.V. and U.S. Philips Corp., in patent litigation, Philips v. Acer Inc., ASUSTeK Computer, Double Power Tech., HTC, Southern Telecom, Visual Land, Zowee Marketing Co., Ltd., Shenzen Zowee Technology Co., Ltd., YiFang USA, Inc. d/b/a EFun, Inc., and Intervenor/Counterclaim Defendant Microsoft Corporation. Civil Actions No. 15-1125-GMS, No. 15-1126-GMS, No. 15-1127-GMS, No. 15-1128-GMS, No. 15-1130-GMS, No. 15-1131-GMS, and No. 15-1170-GMS (D. Del.).

9. Jul. 2017 to Dec. 2018, Technical expert and deponent, for Haynes and Boone, LLP, and mSIGNIA in patent litigation, mSIGNIA v. InAuth. Civil Action No. 8:17-cv-01289-AG-KES (C.D. California).

10. Nov. 2017 to Jun. 2019, Technical expert and deponent, for Thompson & Knight LLP and SEVEN Networks LLC in patent litigation, Seven Networks LLC v. Google, Samsung, and ZTE. Civil Actions No. 2:17-CV-441-JRG, No. 2:17-CV-442-JRG (E.D. Texas), and 3:17-cv-1495-M (N.D. Texas).

11. Jun. 2018 to present, Technical expert, deponent, and testifying witness, for Kramer Levin LLP and Centripetal Networks, Inc. in IPRs and patent litigation, Centripetal Networks, Inc. v. Keysight Technologies, Inc. and Ixia, and Cisco. Civil Action No. 2:17-cv-00383/HCM-LRL (N.D. Virginia, Norfolk Div.). IPR2018-01386 (PTAB), IPR2018-01443 (PTAB), IPR2018-01444 (PTAB), and IPR2018-01512 (PTAB).

12. Apr. 2019 to present, Technical expert for McKool Smith and SEVEN Networks LLC in patent litigation, SEVEN Networks LLC v. Apple, Inc. Civil Action No. 2:19-cv-115 (E.D. Texas).

13. Jun. 2019 to present, Technical expert, for Kramer Levin LLP and CUPP Cybersecurity LLC, in patent litigation, CUPP Cybersecurity LLC, et al., v. Trend Micro, Inc., et al., and CUPP Cybersecurity LLC, et al., v. Symantec Corp. Civil Action 3:18-cv-01251-M (N.D. Tex.), 19-cv-00298 (N.D. Cal.), and 5:18-cv-04720 (N.D. Cal.).