Subject Matter Eligibility Examples: Business Methods

The following examples should be used in conjunction with the *2014 Interim Guidance on Subject Matter Eligibility* (2014 IEG) and the follow-on guidance. As the examples are intended to be illustrative only, they should be interpreted based on the fact patterns set forth below. Other fact patterns may have different eligibility outcomes. While some of the fact patterns draw from U.S. Supreme Court or U.S. Court of Appeals for the Federal Circuit decisions, each of the examples shows how claims should be analyzed under the 2014 IEG. All of the claims are analyzed for eligibility in accordance with their broadest reasonable interpretation. Citations for the cases discussed in these examples are provided in the chart of court decisions available on the Office's website.

Note that the examples herein are numbered consecutively beginning with number 34, because 33 examples were previously issued.

34. System for Filtering Internet Content

The following was a claim found eligible by the Federal Circuit in BASCOM Global Internet v. AT&T Mobility LLC, 119 USPQ2d 1236 (Fed. Cir. 2016) (BASCOM). The patent at issue is U.S. Patent No. 5,987,606. As the claim in this example is eligible, no written analysis would be provided in an Office action. Claim 1 is directed to an abstract idea and has additional elements that amount to significantly more than the abstract idea because they add specific limitations other than what are well-understood, routine, conventional activities in the field and result in an improvement to the technology of filtering content on the Internet. The court's rationale for eligibility is explained below in the context of the 2014 IEG.

Background

Applicant has invented a system for filtering content from an Internet computer network by an Internet Service Provider (ISP) server using individual controlled access network accounts. At the time of applicant's invention in 1997, there was a need to block access to certain web sites for certain end users. For example, a corporation may want to allow access to certain technical or business sites, while blocking access to certain entertainment sites, and a parent may seek to block access by their children to certain objectionable sites.

Previous systems controlled access to content received by client machines over the Internet by filtering the information available using "black-listing" (*i.e.*, preventing access to all web sites on a predetermined list of web sites), "white-listing" (*i.e.*, allowing access to all web sites that are on a predetermined list of web sites), or word-screening or phrase-screening (*i.e.*, preventing access to a web page that contains any word or phrase on a predetermined list). Initially, the filtering software was placed on a client computer. However, this configuration suffered from several disadvantages because the end user could modify or work around the filtering software, the difficulty and time to install on each client computer was great, each client computer required configuration of the software based on its hardware and operating system, and a database storing the allowed or disallowed websites needed to be frequently updated. To overcome the disadvantages of installing the filtering software on a client computer, the filtering software was placed on a local server. In this configuration, client computers on a local area network connected to the Internet through a local server. If an end user on a client computer requested a website on the Internet, the local server would filter all requests for Internet content. This approach suffered from similar disadvantages including being limited to one set of filtering criteria, time-consuming installation and maintenance, and the filtering software being tied to one local area network or local server platform. Finally, ISPs used a server-based configuration in which a filter was installed on their remote servers to prevent

subscribers from accessing certain websites. However, this configuration only allowed for a single set of filtering criteria for all of the subscriber's end users.

In the instant application, applicant's system improves upon the prior art filtering systems by providing a system for filtering Internet content by subscribers on an individually customizable basis. An ISP server stores a filtering scheme in memory and a database of a plurality of sets of filtering elements associated with individual end users. The filtering scheme is executable code, including object code, interpreted code (*e.g.*, Java™ or Javascript™), other high-level code, or a combination thereof. The ISP server associates an end user account with a set of filtering elements from a plurality of filtering elements (*e.g.*, a master list of words or phrases that are not allowed) and one or more filtering schemes (*e.g.*, a word-screening type or phrase-screening type filtering scheme).

In applicant's system, the ISP server receives a log-in request from an end user. After verifying the identity of the end user, the ISP server determines the filtering scheme and filtering elements associated with the end user based on the end user account. The ISP server then receives a request to access a website from the end user and identifies the particular website requested. The ISP server implements the filtering scheme associated with the end user account utilizing the customized filtering elements that are associated with the end user account. The ISP server then determines whether the filtering scheme authorizes the request. If the request is authorized, it is processed and forwarded to the Internet. If it is not authorized, the ISP server provides a rejection notice to the end user.

In one embodiment, a request to access the Internet from an end user is partially processed while the ISP server monitors the content for certain words or phrases using the filtering scheme (*e.g.*, a word-screening or phrase-screening scheme). In this embodiment, the ISP server stores a table of logged-in end users associated with the filtering scheme. The request for Internet access is forwarded directly to the Internet. The ISP server then monitors all data packets transmitted to the ISP server to determine which packets will be forwarded to the end users stored in the table. If a data packet is being sent to a user stored in the table, the ISP server screens the packet based on the filtering scheme and filtering elements associated with that end user's account. If the data packet(s) match the filtering elements of the filtering scheme, such as by containing specific words or phrases, the transmission of the data packet(s) to the user is terminated.

Representative Claim

1. A content filtering system for filtering content retrieved from an Internet computer network by individual controlled access network accounts, said filtering system comprising:

a local client computer generating network access requests for said individual controlled access network accounts;

at least one filtering scheme;

a plurality of sets of logical filtering elements; and

a remote ISP server coupled to said client computer and said Internet computer network, said ISP server associating each said network account to at least one filtering scheme and at least one set of filtering elements, said ISP server further receiving said network access requests from said client computer and executing said associated filtering scheme utilizing said associated set of logical filtering elements.

Analysis

Claim 1: Eligible

The claim recites a local client computer and a remote ISP server that implements at least one filtering scheme and a plurality of sets of logical filtering elements. The system comprises a device or set of devices and, therefore, is a machine, which is a statutory category of invention (*Step 1: YES*).

The claim is then analyzed to determine if the claim is directed to a judicial exception. The claim recites a system for filtering content retrieved from an Internet computer network, which generates access requests for individual accounts, associates each account with at least one filtering scheme and at least one set of filtering elements from a plurality of sets of filtering elements, receives the access requests, and executes the associated filtering scheme utilizing the associated set of filtering elements. Thus, the focus of the claim and its character as a whole is on the idea of filtering content, which is implemented by a system that uses computer and networking components.

Filtering content is according to the court a "method of organizing human behavior" that is similar to other concepts that have been identified as abstract by the courts, such as tracking financial transactions to determine whether they exceed a pre-set spending limit in *Intellectual Ventures I v. Capital One Bank;* 1) collecting data, 2) recognizing certain data within the collected data set, and 3) storing that recognized data in a memory in *Content Extraction;* and organizing information through mathematical correlations in *Digitech*. Therefore, it is reasonable to conclude based on the similarity of the idea described in this claim to several abstract ideas found by the courts that claim 1 is directed to an abstract idea (*Step 2A: Yes*).

This conclusion is not altered by *Enfish*, where the Federal Circuit stated that certain claims directed to improvements in computer-related technology, including claims directed to software, are not necessarily abstract (*Step 2A*). Unlike the claims in *Enfish*, claim 1 is not clearly directed to an improvement in computer-related technology (*e.g.*, computer functionality). Thus, because it is not readily apparent that claim 1 is directed to a non-abstract idea under *Step 2A*, it is necessary to analyze the additional elements in claim 1 under *Step 2B*.

It is noted, however, that the Federal Circuit in BASCOM described claim 1 as presenting a "close call" as to what it is directed to. Thus, if an examiner skilled in this art recognizes that the claim is directed to an Internet-centric problem, for example, or clearly to an improvement in the computer technology of filtering, it would be appropriate to find that the claim, while "involving" an abstract idea is not "directed" to that idea standing alone, thus ending the analysis with a finding of eligibility at Step 2A.

Under *Step 2B*, the claim as a whole is analyzed to determine whether any element, or combination of elements, is sufficient to ensure the claim amounts to significantly more than the abstract idea. The claim recites the additional limitations of 1) controlled access network accounts, 2) a local client computer to generate network access requests for the controlled access network accounts, 3) an Internet computer network, and 4) a remote ISP server coupled to the client computer and the Internet computer network. The remote ISP server associates each account with at least one filtering scheme and at least one set of filtering elements from a plurality of sets of filtering elements, receives the access requests, and executes the associated filtering scheme utilizing the associated set of filtering elements. The local computer, ISP server, Internet computer network, and controlled access network account are generic computer and networking components performing generic computer and networking functions at a high level of generality. As the Federal Circuit determined, these limitations do not amount to significantly more when "taken individually, [because they] recite generic computer, network and Internet components, none of which is inventive by itself."

However, the analysis under *Step 2B* (also called the "inventive concept inquiry") requires more than determining that each additional claim element – the controlled access network accounts, a local

client computer, an Internet computer network, and a remote ISP server – is well known by itself. Here, an inventive concept can be found in the unconventional and non-generic ***combination*** of known elements, and more specifically "the installation of a filtering tool at a specific location, remote from the end-users, with customizable filtering features specific to each end user" where the filtering tool at the ISP is able to "identify individual accounts that communicate with the ISP server, and to associate a request for Internet content with a specific individual account." The Federal Circuit also determined that the claimed arrangement of elements in the system results in an improvement in the technology of filtering content on the Internet, because it offers "both the benefits of a filter on the local computer, and the benefits of a filter on the ISP server."

Further, these limitations confine the abstract idea to a particular, practical application of the abstract idea and, as explained in the specification, this combination of limitations is not well-understood, routine or conventional activity. Unlike the claimed system, previous content filtering systems were able to be modified by end users when the systems were located on local client computers rather than on the ISP server and were dependent on hardware and software on the local computer, or limited to a configuration based on the particular local client computer, local server, or ISP server. In addition, these limitations do not simply recite an instruction to apply the abstract idea of filtering content on the Internet or to perform the abstract idea on a generic set of computers. Instead, the claim recites a "technology-based solution" of filtering content on the Internet that overcomes the disadvantages of prior art filtering systems. Thus, when viewed as an ordered combination, the claim limitations amount to significantly more than the abstract idea of content filtering (*Step 2B: Yes*). The claim is patent eligible.

In practice, if an examiner believes the record would benefit from clarification, remarks could be added to the Office action or reasons for allowance indicating that the claim recites the abstract idea of filtering content. However, the claim is eligible because analyzing the claim limitations as an ordered combination demonstrates that the claim is a particular application of and an improvement to the technology of filtering content on the Internet, rather than well-understood, routine, conventional activity or a simple instruction to apply the abstract idea of filtering content on the Internet or to perform the abstract idea on a generic set of computers.

Additional explanation of prior decisions from *BASCOM*

The following discussion of case law is informative regarding the reasoning that led the court in *BASCOM* to hold claim 1 patent-eligible. It may be useful to examiners to recognize the similarities and differences as identified by the Federal Circuit between claim 1 and the claims at issue in *DDR*, *OIP, Intellectual Ventures I*, *Content Extraction*, *Ultramercial*, and *Accenture*. A discussion of the case law to this extent is not required during examination.

In *DDR*, the claimed invention solved the problem of retaining potential customers on a website by "sending the viewer to a hybrid webpage that combined visual elements of the first website with the desired content from the second website that the viewer wished to access." The claimed invention in *DDR* was not a "business method *per se*." Similarly, even though claim 1 in *BASCOM* was "engineered in the context of filtering content," claim 1 is not simply directed to the abstract idea of filtering content applied to the Internet, *i.e.*, abstract idea + "apply it". Instead, claim 1 recites a "technology-based solution" of filtering content on the Internet that overcomes the problems in the prior art with other Internet content filtering systems rather than "an abstract-idea-based solution" (*i.e.*, a solution "implemented with generic technical components in a conventional way").

In contrast, in *OIP*, the claims were directed to the performance of the abstract idea of price optimization on generic computer components using conventional computer functions. In other words, the claimed invention was "simply the generic automation of traditional price-optimization

techniques" and was not a "technology-based solution" of the abstract idea. Claim 1 of *BASCOM* presents a "technology-based solution" of filtering content on the Internet that overcomes the problems in the prior art with other Internet content filtering systems as discussed above.

Finally, the claims in *Intellectual Ventures I*, *Content Extraction*, *Ultramercial*, and *Accenture* are directed to an abstract idea performed on generic computer components, "without providing a specific technical solution beyond simply using generic computer concepts in a conventional way." In *Intellectual Ventures I*, the claims were directed to the abstract idea of tracking financial transactions to determine whether they exceed a pre-set spending limit simply implemented on a generic computer and the Internet. In *Content Extraction*, the claims were directed to the abstract idea of collecting data, recognizing certain data within the collected data set, and storing that recognized data in a memory performed on generic scanning devices and computers. In *Ultramercial*, the claims were directed to the abstract idea of using advertising as an exchange or currency on the Internet. And finally, the claims in *Accenture* were directed to the abstract idea of generating rule-based tasks for processing an insurance claim using generic computer components performing conventional activities. Unlike the claims in *Intellectual Ventures I*, *Content Extraction*, *Ultramercial*, and *Accenture*, claim 1 of *BASCOM* is not simply directed to the abstract idea of filtering content on the Internet or on generic computer components performing conventional activities. Instead, claim 1 "carve[s] out a specific location for the filtering system (a remote ISP server) and require the filtering system to give users the ability to customize filtering for their individual network accounts."

35. Verifying A Bank Customer's Identity To Permit An ATM Transaction

The following fact pattern and claims are hypothetical. Assume that the claims are presented in a recently filed application that is under examination and thus each claim is given its broadest reasonable interpretation in view of the specification as it would be understood by one of ordinary skill in the art. In this example, the terms in the claim are given their plain meaning in the art because no special definitions have been set forth in the specification. An abbreviated version of the hypothetical specification is provided below. Claim 1 is ineligible, because it is directed to an abstract idea and does not recite additional elements that amount to significantly more. Claims 2 and 3 are directed to the same abstract idea, but are eligible because they have additional elements that amount to significantly more than the abstract idea (i.e., provide an inventive concept) because they implement the abstract idea with specific meaningful limitations.

Background

Financial institutions routinely provide automated teller machines (ATMs) for customers to conduct banking transactions at convenient locations other than brick-and-mortar banks, and without the need to interact with a bank teller. Typical ATMs include a customer interface with a keypad, function key, display, outlet slot for statements or other information, cash dispenser slot, deposit inlet, and often a speaker to provide customer voice guidance and a camera to monitor transactions. A reader is provided for customers to present data bearing records, which can include data corresponding to the customer, financial accounts, or other data, and are commonly embodied as a bank card with a magnetic strip or a contactless card with a radio frequency identification (RFID) tag. Other input devices, such as a biometric reader to receive customer identifying inputs such as fingerprints, iris scans, and face topography data, a camera, or speech recognition device, used to identify a user can be provided as well. The customer interface is coupled to a controller with a processor and memory and a network communicator to enable communication between the controller and a financial institution to exchange information about the transactions. To conduct a transaction, a customer typically inserts a bank card into the appropriate slot in the ATM and inputs a personal identification