UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* DAVID G. KUEHR-McLAREN,
MARTIN PRESLER-MARSHALL,
CALVIN S. POWERS,
TIMOTHY SHORIAK, and
JOHN H. WALCZYK, III

---

Appeal 2008-2084
Application 10/706,464
Technology Center 3600

---

Decided: August 28, 2008

---

Before HUBERT C. LORIN, LINDA E. HORNER, and
MICHAEL W. O'NEILL, *Administrative Patent Judges*.

LORIN, *Administrative Patent Judge*.

## DECISION ON APPEAL

## STATEMENT OF THE CASE

David G. Kuehr-McLaren, et al. (Appellants) seek our review under 35 U.S.C. § 134 of the final rejection of claims 1-12. We have jurisdiction under 35 U.S.C. § 6(b) (2002).

## SUMMARY OF DECISION

We AFFIRM.[1]

## THE INVENTION

The invention "relates to the use of privacy policies in computer-based on-line commerce in which sellers and buyers of goods or services are linked via an electronic marketplace where deals are negotiated and consummated." (Specification 1:11-13.) A drawback in the convenience and enjoyment of e-commerce is the need to submit private information. (Specification 2:11-12.) The invention seeks to overcome this drawback by having participants

> involved in transacting business in an E-marketplace (E-marketplace participants) each identify and submit to the E-marketplace relevant characteristics related to their privacy policy needs (those that they adhere to, referred to as "privacy policies"; those that they require, referred to as "privacy preferences", or both). Typically, this

[1] Our decision will make reference to Appellants' Appeal Brief ("Br.," filed Oct. 10, 2006) and the Examiner's Answer ("Answer," mailed Mar. 19, 2007).

> would occur during the registration process when an E-marketplace participant first registers with the E-marketplace … .

(Specification 5:2-7.) "The privacy policies and privacy preferences of the E-marketplace participants are then matched up, and those with matching characteristics are given access to each other, while those that do not match up are either [*sic*] denied access. This serves as a search filter to match up consumers with providers." (Specification 5:8-11.) In so doing, the invention prevents transactions between participants in the E-marketplace from going forward unless a participant's privacy-use information matches that of another. (Specification 9:3-12.)

Claim 1, reproduced below, is illustrative of the subject matter on appeal.

> 1. A method of conducting electronic commerce transactions among participants in an E-marketplace, comprising the steps of:
>
> obtaining privacy-use information for each participant;
>
> comparing the privacy-use information for each participant to determine matches; and
>
> only allowing transactions to occur between participants who have matching privacy-use information.

## THE REJECTIONS

The Examiner relies upon the following as evidence of unpatentability:

| | | |
|---|---|---|
| Epling | US 2005/0091101 A1 | Apr. 28, 2005 |

The following rejection is before us for review:

1. Claims 1-12 are rejected under 35 U.S.C. § 102(e) as being anticipated by Epling.

## ISSUES

The issue before us is whether the Appellants have shown that the Examiner erred in rejecting claims 1-12 under 35 U.S.C. § 102(e) as being anticipated by Epling. The Appellants contend that Epling does not allow transactions to occur *only* if the privacy use information for each participant matches. The issue turns on the construction to be given the last step of claim 1 and, in light of that construction, whether Epling describes prohibiting a participant from making a transaction where the participant's privacy-use information does not match that of the other participant in the transaction.

## FINDINGS OF FACT

We find that the following enumerated findings of fact (FF) are supported by at least a preponderance of the evidence. *Ethicon, Inc. v. Quigg*, 849 F.2d 1422, 1427 (Fed. Cir. 1988) (explaining the general evidentiary standard for proceedings before the Office).

*Claim construction*

1. Claim 1 is drawn to a method of "conducting electronic commerce transactions among participants in an E-marketplace."
2. The Specification does not provide an express definition for "E-marketplace" but describes it as "a standard form of conducting . . . business" (Specification 2:2-3) and which common e-commerce

sites on the Internet provide "as a central location for negotiation of sales and/or auctions of products or services from a seller to a consumer (e.g., bidders)" (Specification 2:6-8). The Specification (referring to Fig. 1 at 7:5-8) further states:

> Typically, the E-marketplace 100 will comprise a server configured to receive communications from the network connections 102, 112, store information for viewing by parties connected to the network connections 102 and 112, and store other information pertaining to transactions which may occur in the E-marketplace.

3. Accordingly, an "E-marketplace" encompasses, for example, a server computer networked with computers of users conducting business.
4. Participants in an E-marketplace include users of computers conducting business.
5. The method of claim 1 comprises three steps but does not require a structural connection between any of the three steps and any element of the E-marketplace.
6. Claim 1 encompasses conducting the three recited steps independent of the physical operation of the E-marketplace.
7. Claim 1 does not specify who or what conducts the recited steps of the method.
8. Step 1 of the claimed method calls for "obtaining privacy-use information for each participant [in the E-marketplace]." The claim does not limit the means by which the privacy-use information for each participant is obtained.

9. Privacy-use information could be obtained through human interaction, including via a purely mental step.
10. Step 2 of the claimed method calls for "comparing the privacy-use information for each participant to determine matches." The claim does not limit the means by which the privacy-use information for each participant is matched.
11. Step 2 could be performed through human interaction alone, including via a purely mental step.
12. Step 3 of the claimed method calls for "only allowing transactions to occur between participants who have matching privacy-use information." The claim does not limit the means by which transactions between participants who have matching privacy-use information are only allowed to occur.
13. Step 3 could be performed through human interaction alone, including via a purely mental step.
14. "Privacy-use information" refers to the "privacy policies and privacy preferences of the E-marketplace participants." (Specification 5:8-9; see also 6:14-15.) This may include "the seller's policy regarding sale of email lists, use of sales information, protection of credit card numbers and other personal information, demographic information and the like." (Specification 8:6-8.) Alternatively, this may include "[buyer] decisions regarding use of private information such as email address, name and address information, credit card information and any other personal or business-related information that could be considered private." (Specification 8:13-15.)

15. Accordingly, "privacy-use information" covers a broad spectrum of information that E-marketplace participants may wish to keep private.

*The prior art*

16. Epling relates to a method for presenting privacy policies to a computer user according to a computer user's preferences. "Systems and methods are described for evaluating Web site privacy policies and transforming the policy data into a user-centric view for presentation to a user according to a set of concerns designated by the user." (Epling [0009].)

17. Epling describes networked server computers as exemplary systems for implementing its method. (See Epling [0060] and [0069].)

18. Epling describes a business environment. (See Epling [0004] and [0018].)

19. One of ordinary skill in the art reading Epling would understand that computer users are needed to operate Epling's system.

20. Since Epling describes its system in a business environment, one of ordinary skill in the art reading Epling would understand that the computer users needed to operate Epling's system in a business environment would include participants in the transacting of business.

21. The Examiner pointed to block 208 of Fig. 1 and [0038] of Epling as evidence that Epling describes comparing a computer user's privacy-use information with the privacy policies of websites. (Answer 5.)

22. Referring to Fig. 1, Epling [0038] reads, in part, as follows:

> At block **208**, the trust engine **116** compares the concerns **120** with the statements **112** included in the privacy policy file **110**. The comparison is a standard Boolean match procedure which attempts to match keywords or tags included in the concerns **120** file with metatags included in the policy statements **112**.

23. "[C]oncerns **120** are a list of one or more privacy concerns identified by the user." (Epling [0027].)

24. The set of concerns that a user might identify include "personal private data." (Epling [0018].) "Any personal data that a user would typically like to protect from misuse and abuse qualifies as personal data as used herein." (Epling [0018].)

25. Statements 112 and privacy profile file 110 are parts of a Web page or included as part of a Web site. (Epling [0024].)

26. Accordingly, the Examiner's reading of Epling as describing comparing a computer user's privacy-use information with the privacy policies of websites is accurate.

27. The Examiner relied on Epling [0043] as evidence that Epling describes "only allowing transactions to occur between participants who have matching privacy-use information because a user is barred from browsing a web site and notified in a[n] indicator that their privacy policy does not match that of the web sites." (Answer 5.)

28. Epling [0043] reads (referring to Fig. 2):

> If the comparison turns up any matches ("Yes" branch, block **214**), then an indicator is set at block **216**. This indicator may be a small icon

> placed on a toolbar of the user's display, or it could be a popup box configured to really get the user's attention. If no matches are found – indicating that the Web site privacy policies do not conflict with the user's concerns – ("No" branch, block **214**), then the user continues to browse the site at block **224**.

29. Epling [0044] further states (referring to Fig. 2):

> At block **218**, the user may then opt to see the results by responding to the notification set in block **216** by, for example, clicking on a notification icon or responding to a popup box. If the user wants to see the results of the comparison ("Yes" branch, block **218**), then the results are displayed by the UI module **122** at block **220**. If the user does not want to see the results ("No" branch, block **218**), then the user continues to browse the site at block **224**.

30. As noted in the Answer (p. 6), Epling [0057] further states:

> As a result of the processes described in **FIG. 2** and **FIG. 3**, the user is presented with a set of user-focused privacy concerns instead of a company-based set of privacy concerns. As a result, furtive attempts to hide unpopular usage of personal data are defeated and the user can quickly determine if the user wants to access the Web site.

31. Epling [0044] and [0057] describe providing the user the option of *not* proceeding to the Web site whose privacy policies do not match the user's privacy concerns.

## PRINCIPLES OF LAW

*Anticipation*

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987).

## ANALYSIS

The Appellants argued claims 1-12 as a group (Br. 4-7). We select claim 1 as the representative claim for this group, and the remaining claims 2-12 stand or fall with claim 1. 37 C.F.R. § 41.37(c)(1)(vii) (2007).

The Examiner relied on certain passages in Epling as evidence that Epling describes a method that compares a computer user's privacy concerns with the privacy policies of Web sites and providing the user the option of *not* proceeding to the Web site whose privacy policies do not match the user's privacy concerns. (Answer 5-6.) (See FF 21, 27, and 30.) We find that Epling describes such a method. (FF 16-31.)

There is no dispute that Epling describes matching a user's privacy concerns and a Web site's privacy policy. The Appellants conceded that Epling (at [0044]) shows the user is presented with a list of security concerns and that this list is compared to a privacy listing of a website. (Br. 5, last 4 lines.)

The dispute is over whether Epling's description of a method whereby the user is given the option of *not* proceeding to the Web site whose privacy policies do not match the user's privacy concerns meets the claim limitation "*only* allowing transactions to occur between participants who have matching privacy-use information" (claim 1; emphasis added).

According to the Appellants, Epling does not allow transactions to occur *only* if the privacy use information for each participant matches.

> The Examiner asserts that Epling teaches comparing the privacy use information for each participant to determine matches as well as only allowing transactions to occur between participants who having matching privacy use information. The Examiner is incorrect in this assertion. Epling does in fact allow transactions to occur between participants who have non-matching privacy use information, specifically stating so in the explanation of Figure 2 (in particular, paragraphs [0044] and [0050]).

(Br. 5.) The Appellants argued that, in Epling, "the user is presented with the option to view the results or to continue on to the web site. If the user opts to continue to the web site, the user never sees the results and therefore can access the web site even if the privacy use information does not match." (Br. 6.) "In the present invention, the user is not even provided the option of participating in a transaction where the privacy-use information . . . are made available to the user." (Br. 6.)

We are not persuaded by the Appellants' argument.

The Appellants' characterization of the Epling method as one that gives the user the *option* to access a web site even if the user's privacy concerns do not match the web site's privacy policy is correct. (FF 28-30.) But the claimed step of "*only* allowing transactions to occur between participants who have matching privacy-use information" reads on a user selecting the option to not access a web site if the user's privacy concerns do not match the web site's privacy policy.

Epling [0057] states that "the user can quickly determine if the user *wants to access* the Web site" (emphasis added) based on the results of the Epling privacy-use matching process. Accordingly, we agree with the Examiner that Epling's process gives the user the option *not* to access a web site if the user's privacy concerns do *not* match the web site's privacy policy. In making the decision not to access a web site if the user's privacy concerns do not match the web site's privacy policy, a user practicing the Epling method necessarily puts him or herself in the position to decide to *only* allow him or herself to access a web site if the user's privacy concerns *match* the web site's privacy policy.

The Appellants' argument that "[i]n the present invention, the user is not even provided the option of participating in a transaction where the privacy-use information does not match as only participants with matching privacy-use information are made available to the user," (Br. 6) suggests the Appellants are construing the claimed step of "only allowing transactions to occur between participants who have matching privacy-use information" as restricting a user's future option to participate in a transaction until participants' privacy-use information match. This implies the use of a means for continually monitoring participation between participants and controlling the participation depending on the results of the matching step. But no such means is recited in the claim. The scope of the claim is such that it encompasses permitting a user to determine whether to allow particular transactions to proceed if his/her privacy-use information matches that of a website. If a user determines for him or herself to not allow transactions to proceed because his or her privacy-use information does not match that of a website, the user has necessarily made the decision to "only

[to] allow[ ] transactions to occur between [the user and the website] who have matching privacy-use information (claim 1)." Accordingly, since Epling describes giving a user the option to proceed if his or her privacy-use information matches that of a website, Epling reads on the claimed method whereby users decide to "only [to] allow[ ] transactions to occur between [the user and the website] who have matching privacy-use information" (*id*.)

There being no other arguments challenging the rejection, we will sustain the rejection.

## CONCLUSION

We conclude that the Appellants have not shown that the Examiner erred in rejecting claims 1-12 under 35 U.S.C. §102(e) as being anticipated by Epling.

## DECISION

The decision of the Examiner to reject claims 1-12 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv) (2007).

## AFFIRMED

hh

(SAUL-RSW) PATENT DOCKETING CLERK
IBM Corporation (SAUL-RSW) C/O Saul Ewing LLP
Penn National Insurance Tower
2 North Second Street, 7th Floor
Harrisburg, PA  17101