

TYPES NOT MAPPED YET December 31, 2020 | TTR not mapped yet | Mark Sableman

Use of fake identities found deceitful in commercial email – why not elsewhere on the Internet?

The Third Circuit Court of Appeals recently had to decide a sensitive and difficult issue: Can you use a false identity to deceive someone when you are selling something by email? After careful deliberation, the court held that under the federal CAN-SPAM Act, such conduct was both criminal and deceitful.

Not a big deal. Deceit has always been unlawful. Of course you can criminalize deceit. But why was the decision so sensitive and difficult? Because it involved modern talismanic concepts: use of anonymity and false identities on the Internet.

Many people today believe that everyone has an absolute right to cloak his or her identity on the Internet. Thus, the judges on the Third Circuit panel, in [Rad v. Attorney General](#), felt they had to tread carefully in burdening the use of anonymity or false identities on the Internet, because of “troubling constitutional and practical consequences.”

In *Rad*, a non-U.S. citizen who had been convicted of violating the CAN-SPAM Act in connection with a penny stock scheme was ordered expelled from the country. He challenged this ruling, claiming that his conviction didn’t involve fraud or deceit (the justification, under immigration laws, for his expulsion order). This forced the Third Circuit to examine certain provisions of CAN-SPAM, the federal law regulating unsolicited commercial email.

Rad was convicted of conspiracies based on his sending of “misleading spam emails,” and, more specifically, using false email name headers, and false references to his own domain. Essentially, he sent emails that falsely identified their origin, presumably to make his operation look more credible than it was. His crime, under CAN-SPAM, was, essentially, using false identities.

The court was concerned because of the extensive use of anonymity and false identities on the Internet, and judicial protection of such uses, all based on a U.S. Supreme Court decision, [McIntyre v. Ohio Elections Commission](#). In that decision, breaking with past decisions that recognized a First Amendment right of anonymity only for dissidents and minorities who legitimately feared retaliation for participation in public debate, the Supreme Court suggested that everyone has a right, in all cases, to cloak his or her identity.

That statement was “dictum” – a statement that goes beyond the determinative issue of the case, as distinguished from the “holding” that was essential to the court’s ruling. Dictum isn’t precedent and needn’t be followed by other courts. But the McIntyre dictum has been followed as if it were sacred scripture. And while the dictum came from a pre-Internet (1985) ruling, it has been applied extensively in the Internet era, to significantly shield anonymous and pseudonymous Internet speakers.

That is why the Third Circuit tiptoed so carefully around interfering with customary Internet anonymity or pseudonymity. In many situations, people regularly use pseudonyms or even false names. Email addresses, for example, often use nicknames, allusions, jokes, abstractions, or other non-legal names. Similarly, domain names rarely use a person or company’s full legal name, and many domain name owners even hide their identity through proxy registrants.

So the Third Circuit asked whether *Rad*’s false email identification was any different from typical Internet naming techniques (like using shorthand phrases on emails and domain names) and practices (like using proxy domain registrants).

The court found that CAN-SPAM doesn’t impose a blanket prohibition on all names that are different from the sender’s legal name. Rather, it prohibits “materially falsified” header information, which means names altered or

concealed in a manner that would deceive the recipient (specifically, by impairing the recipient's ability to identify the true sender).

For that reason, the court found that CAN-SPAM didn't interfere with "longstanding norms," such as shorthand or nickname email addresses. It addressed instead truly misleading and deceitful falsifications, in situations where the truthful information would have made a difference. Presumably, in the Rad case, investors would not have trusted Rad's emails if they had been labeled with his name rather than the falsified names he used.

Ultimately, the court found that Rad was properly expelled from the country, since his CAN-SPAM crime, of falsifying his identity in the emails he sent out, was one of fraud and deceit.

The most interesting part of the Rad ruling is what it would mean if the court's basic insight – that use of fake names can be deceitful – were more widely recognized.

The elephant in the Third Circuit courtroom was the widespread use of anonymity and false identities in social media and message boards to spread disinformation and change the course of events. This extensive use of anonymous and false identities is, on the whole, just as deceitful as the conduct at issue in Rad, and has far greater consequences. (As just one example, we covered the impact of disinformation on the election process during our ["Muting Misinformation" blog series](#) this past summer.)

While some of those who shield their identities on the Internet do so for the reasons that were protected even before McIntyre (because they are minorities or dissidents who have important things to express and a legitimate fear of retaliation), false identities are often used for outright deceit, similar to what occurred in the Rad case.

Disinformation machines, domestic as well as foreign, use false identities, quite successfully, to deceive customers, citizens, and voters. Russian disinformation in the 2016 election, for example, was notably successful with its social media posts using fake domestic identities, thereby deceiving voters into accepting views that they felt came from their neighbors, or, alternatively, rejecting views that they thought came from other Americans.

Yet, the current ethos is so strong that all anonymity and false identities must be protected, that many people believe that even deliberate disinformation, powered by deceitful false identities, is constitutionally protected. We saw that, for example, when one of the consultants to the Senate Intelligence Committee actually stated in a report, "we respect the privacy of fake people."

The Third Circuit's decision in Rad reminds us that deceit is bad. Deceitful use of false identities, or concealment of true identities, is a form of fraud and deceit. Deceit is not a form of free speech; it is a misuse of speech. It should be punished, not celebrated or protected.

Rather than start from the overbroad presumption in McIntyre that all anonymity and false identities are allowable, future cases involving use of fake identities in social media and in disinformation campaigns should start from the simple and unarguable holding of Rad, that material and harmful deceit can and should be prohibited and prosecuted.

[Mark Sableman](#) is a member of Thompson Coburn's Media and Internet industry group, and a member of the Firm's Intellectual Property practice group.

authorsTest



mark

Mark Sableman