

“Cyberlibel”: You *Can* Fight Back

By David A. Potts

An astounding new information technology sweeps the globe, changing the way we communicate, conduct business and live our lives. Tremendous potential is unleashed; not least, the hope of drawing a fractured humanity together through the instantaneous exchange of knowledge and experience. So too, as always happens with such breakthroughs, emerges the potential for outright malice. And so it goes: Observers quickly detect misinformation being disseminated through this stunning innovation. Fraudsters pounce, falsehoods race around the world, reputations are ruined.

You might think that all this describes the dawn of the Internet age. But think again: It is 1846, and the advent of *the telegraph*. As superbly recounted in Tom Standage's *The Victorian Internet*, lawyers and the courts would come to grapple with entirely new realms of jurisprudence in confronting the use of the telegraph to spread falsehoods and innuendo on a scale, and with a reach, never before seen. This would eventually lead to the accumulation of case law to inform the legal methods used to combat, and ultimately rein in, defamation-by-telegraph.

Fast-forward to 2011, and the era of Wikileaks, online jihadist recruitment and Facebook-led revolutions, among many other strange manifestations of the Internet era, in which some 1.9 billion people are interconnected in more than 190 countries. Here again, few understand the forces that have been unleashed. Fewer still know how to control them. Most assume we can't control them at all. In fact, on matters of organizational reputation, many people have concluded that once you are slagged in cyberspace it's just "out there" and it cannot be taken back. Yet just as the dawn of the telegraph more than 150 years ago marshalled the finest legal minds over the challenge of internationally-transmitted libel and slander, a new field of Internet defamation case law is struggling to emerge that will point the way to an entire arsenal of defences and methods of recourse.

That said, the legal community worldwide has barely scratched the surface of some baffling questions. Among them: What are the differences between defamation in cold, hard print and defamation in the viral online environment? Do these differences, in turn, call for different strategies and tactics, reflecting a new kind of "informational warfare"? How can we reconcile the jurisdictional variances governing defamation law in the country of origin versus the country (or countries) of dissemination? What of the reality that in the mainstream media defamers are generally identifiable, while online culprits are often anonymous? How to establish editorial rules of conduct in an unstructured, universally-accessible realm where the producers of the information and its consumers can effortlessly slip from one role into the other? How to apportion liability between the original publication of the libel and the near-limitless avenues for

republishing through hyperlinks? To what extent do the many ISPs and search engines involved share in the liability for disseminating a falsehood? How do all these variables influence the courts (wherever they may be) in awarding damages in cyberlibel actions? And ultimately, how can these judgments be enforced?

Even then, once all these issues are digested and factored into a potential legal and reputational defence, there remains a final and critical question: Will the online reaction to your counter-measures provoke even broader dissemination of the offending content, propelled by new and more vitriolic comment? This is an entirely separate consideration, to be approached with a blend of legal sophistication and something approaching the measures used in guerrilla warfare.

The answers to these confounding questions, and the legal methodologies that are slowly beginning to arise from them, are of vital concern not just to defamation lawyers, but to all interests with a stake in reputation management. They include corporate officers, professional associations, government officials, crisis response practitioners, prominent public figures and many others. After all, another organizational discipline has come to the fore in recent years known as risk management. The “goodwill” associated with an entity’s reputation is today no longer an intangible asset but a concrete number on the balance sheet. It can take years to build that brand equity. In the age of cyberlibel, it can be vaporized at the push of a button. So it falls to this generation of legal minds to consolidate the case law, innovate using new approaches, learn from history, and fight back in this new environment, just as our forebears did more than a century and-a-half ago.

To be sure, our Victorian ancestors would have been impressed by – and perhaps even fearful of – many of the marvels of our age, such as rockets to the moon and talking cars. But not by the Internet. As Tom Standage reminds us, they had their own.

David A. Potts is a Toronto lawyer specializing in defamation law and the author of *Cyberlibel: Information Warfare in the 21st Century?*, published by Irwin Law.