ONLINE PRIVACY AND ONLINE SPEECH: THE PROBLEM OF THE HUMAN FLESH SEARCH ENGINE

Weiwei Shen*

I. INTRODUCTION

The *Human Flesh Search Engine* is a literal translation of the Chinese words *Ren Rou Sou Suo Yin Qin* (人肉搜索引擎). It is the collaborative Internet phenomenon of searching for personal information using a combination of human and artificial intelligence. Normally, the human flesh search engine is launched in public online

* SJD student at the University of Pennsylvania Law School. The author would like to thank Professors Matthew Adler, Anita Allen, Joshua Getzler, Seth Kreimer, Sophie Lee, Jacques deLisle, Gideon Parchomovsky, Christopher Yoo, as well as the participants of the 2016 Comparative Constitutional Law Conference at University of Toronto for their helpful comments on earlier drafts.

forums, where Internet users post various kinds of personal information about the victims, such as their names, phone numbers, email addresses, physical addresses, photos, and affiliations.[1] Often, these victims will then be exposed to ethical critiques, public humiliation, or even physical assault.

As opposed to commonly known search engines such as Google, Baidu and Bing,[2] the human flesh search engine uses a network of Internet users to conduct a search. There are features of the human flesh search engine that make it a unique Internet phenomenon. First, Internet users often employ it in response to a wide range of social and political issues, such as government corruption, moral debate, patriotism, or celebrity gossip.[3] Second, using the power of networked Internet users, the collection and analysis of personal information can be conducted much more effectively than traditional search engines. Such personal information, once available, can be rapidly distributed online, making it a powerful mass medium. Third, with the use of the Internet, the human flesh search engine can easily mobilize thousands of Internet users, making it very likely that there are some insiders who can provide the targets' personal information without their consent or knowledge.

It should be noted that despite its nefarious uses, the human flesh search engine can be used for good, such as reuniting families after a natural disaster. However, in most cases, the human flesh search engine is used to expose targets to public humiliation, be they public figures or private individuals. This Note will focus on the

---

[1] The earliest known use of this term dates back to 2001, when a man posted a thread on one of the most popular forums on the Chinese Internet, mop.com, seeking relationship advice. The thread included the picture of a beautiful young woman, who was claimed to be his girlfriend. Suspicious Chinese Internet users employed the human flesh search engine to identify the young woman was actually a young model, Chen Ziyao. *See "Human Flesh Search Engine": An Internet Lynching?*, XINHUA NEWS AGENCY (新华社) (Jul. 5, 2008), http://www.china.org.cn/china/features/content_15959669.htm [https://perma.cc/3RZK-46W3] (describing the idea of a search engine comprised of thousands of Internet users intent on achieving a single goal and providing illustrative examples, including its origin).

[2] *Id.*

[3] For examples of the human flesh search engine, see Celia Hatton, *China's Internet Vigilantes and the 'Human Flesh Search Engine,'* BBC (Jan. 28, 2014), http://www.bbc.com/news/magazine-25913472 [https://perma.cc/4FCG-YRDD] (describing the dedication of the members of the human search engine and the humiliation of the targets).

latter in order to highlight the tension between the right to privacy and the right to free speech in the Internet age.[4]

Privacy and the right to free speech can be thought of as distinct topics, but they frequently collide where the Internet is concerned.[5] On the one hand, many fragments of personal information about individuals are being collected by new technologies, then saved in databases and scattered across the Internet. These fragments of information are permanent, searchable, and subject to computerized cross-reference and retrieval. On the other hand, society is horrified by stories of private photos leaking, cyber-bullying, cyber-stalking, cyber-harassment, and offensive online speech. With the increase in the number and diversity of Internet users, the informal governance mechanisms that have previously governed the Internet are quickly being shown to be inadequate.[6] Therefore, it is necessary to carefully explore the tension between privacy and speech on the Internet with regard to the kind of theoretical structure for legal remedies available.

By examining the human flesh search engine, this Note attempts to explore the tension between privacy and free speech on the Internet. In particular, it focuses on the Wang Fei case—the landmark case of the human flesh search engine in China. The human flesh search engine and the Wang Fei case have implications in both American and Chinese legal systems. They represent universal

---

[4] Public figures were involved in the human flesh search engine usually because of misbehavior or corruption. *See* Sky Canaves, *"Human Flesh Search Engines" Set Their Sights on Official Misbehavior*, WALL ST. J. CHINA REAL TIME REPORT BLOG (Dec. 29, 2008, 6:57 AM), http://blogs.wsj.com/chinajournal/2008/12/29/human-flesh-search-engines-set-their-sights-on-official-misbehavior [https://perma.cc/WP2R-FN5F] (reporting that in 2008 a human flesh search engine conducted a search on a public official in Shenzhen after he was caught on video assaulting a young girl at a restaurant); Jessi Levine, *What Is a "Human Flesh Search," and How Is It Changing China?*, ATLANTIC (Oct. 5, 2012), http://www.theatlantic.com/international/archive/2012/10/what-is-a-human-flesh-search-and-how-is-it-changing-china/263258/ [https://perma.cc/FM3T-NWFP] (reporting that in 2012, Chinese Internet users conducted a human flesh search against a public official, Yang Dacai, after he was found wearing a luxury watch during an inspection for a natural disaster. Yang Dacai was later sentenced to fourteen years in prison for bribery).

[5] The right to privacy has different meanings in the legal academia. This Note limits the inquiry to privacy protection as a way to control dissemination of personal information and excludes the discussion of privacy protection as decisional autonomy.

[6] CHRISTOPHER S. YOO, THE DYNAMIC INTERNET: HOW TECHNOLOGY, USERS, AND BUSINESSES ARE TRANSFORMING THE NETWORK 82–88 (2012) (elaborating on how the informal Internet governance mechanisms were replaced by more formal Internet governance in three contexts: spam control, the domain name system, and congestion management).

problems regulating privacy and free speech, and trigger an issue which both legal systems have not yet squarely addressed—that is, whether the value of privacy outweighs the value of free speech if the underlying online speech is about private individuals (as opposed to public officials and celebrities) and of private concern (as opposed to public concern). This Note examines this issue through the lens of the American legal framework. Drawing on a comparative analysis, this Note attempts to answer the following questions: how should the American legal system respond to the tension between privacy and free speech in the context of the human flesh search engine? What kinds of remedies can each jurisdiction offer to the victims of the human flesh search engine? Finally, what can Chinese policy makers learn from the American legal experience, and how can they provide a more cost-effective regulatory framework?

Part II of this Note begins with an overview of the human flesh search engine, and an analysis of the Chinese court's decisions of the Wang Fei case. This Note uses this case study to reflect on the differences between Chinese and American cultures, and their individual views on privacy and free speech in the Internet.[7]

In the following section (Part III), this Note attempts to demonstrate how the Internet makes previously clear doctrines seem doubtful, and bends well-settled legal principles about free speech and privacy from the pre-Internet age. In particular, this Note will draw distinctions between online speech and off-line speech, speech about private individuals and speech about public officials, and speech of private concern and speech of public concern. This Note argues that when conducting First Amendment analyses on the human flesh search engine, privacy values should trump free speech values if the online speech involved a matter about private individuals of private concern.

In Part IV, I discuss possible tort liabilities and related legal remedies that could arise in human flesh search engine related cases. This Note will mainly focus on the liability of Internet intermediaries in the human flesh search engine, with United States' Section 230 of Communication Decency Act as the primary frame of reference.

---

[7] Sometimes, both of these values achieve the same end. For example, both embrace anonymity and private speech as ways to check unreasonable governmental surveillance. Talley v. Cal., 362 U.S. 60, 64–5 (1959); Lamont v. Postmaster General, 381 U.S. 301, 305–7 (1965); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995). But more often, privacy and free speech are competing interests.

Part V highlights the positive and negative lessons from American jurisprudence. These lessons will then be the basis of recommendations for the Chinese legislature and courts. American courts, legislatures, administrative agencies, technologists and entrepreneurs provide a sophisticated picture of solutions to online privacy infringement. China can learn a great deal from them. In particular, restrictions on online speech should be narrowed more to restrictions on speech about private individuals and of private concerns. On the other hand, the United States has been leaning towards providing absolute immunity to Internet intermediaries, potentially leaving victims of online infringement unprotected. This Note cautions against that. Drawing on a comparative analysis, this Note suggests reforms for the regulation of the human flesh search engine in China. Given the institutional landscape and realities in China, this Note argues that a well-designed notice-based liability regime for an Internet service provider is a more cost-effective approach to address the problems of the human flesh search engine. This Note will also suggest that Internet intermediaries shall be incentivized to cooperate with victims and law enforcement agencies in order to achieve an optimal mechanism. The conclusion sets out final remarks.

II. THE HUMAN FLESH SEARCH ENGINE AND THE WANG FEI CASE

A. Why the Human Flesh Search Engine Is Popular in China

In the past decade, there has been an increasing number of cases related to the human flesh search engine in China. One might ask: why has the human flesh search engine become such a popular Internet phenomenon in China? Before we begin our discussion, it should be noted that online personal information collection and cyber harassment are not uniquely Chinese Internet phenomena. In the United States, "doxing," derived from the word "document tracing," is a similar Internet phenomenon. It refers to the process of gathering, deducing or publishing individuals' information such as name, date of birth, email, physical address, telephone number, photographs,

medical information, etc.[8] The variance in American and Chinese Internet culture accounts for the differences between the human flesh search engine and doxing.

As the first instance of these variations, the demographics of Internet users vary widely by country. After surpassing United States in the number of Internet users (253 million) in 2008,[9] China continued to increase its advantage in that number. In 2015, the number of Internet users in China hit 706 million, almost equal to the combined total of the Internet users in India (354 million), United States (284 million), and Japan (115 million).[10] Moreover, according to a recent survey, Internet users in China are, on average, much younger than their United States counterparts.[11] With more spare time to be spent online and lower mental maturity, younger Internet users are more likely to participate in public opprobrium and be provoked by aggressive language during the course of the human flesh search engine.

Second, the Internet, as a novel form of media, plays a significant role in spreading information about controversial issues in China. Because of the large number of Internet users, bulletin board systems ("BBS") are much more popular on the Chinese Internet than the American Internet. The dearth of contentious and controversial

---

[8] According to the U.S. Federal Bureau of Investigations, "doxing" is the release of "identifying information including full name, date of birth, address, and pictures typically retrieved from the social networking site profiles of a targeted individual." FEDERAL BUREAU OF INVESTIGATION, LAW ENFORCEMENT AT RISK FOR HARASSMENT AND IDENTITY THEFT THOUGH "DOXING" 1 (2011). The most famous doxing case in the United States, by far, is the so-called "Gamergate", which is about the harassment of several women in the gaming industry online. *See* Jay Hathaway, *What Is Gamergate, and Why? An Explainer for Non-Geeks*, GAWKER (Oct. 10, 2014), http://gawker.com/what-is-gamergate-and-why-an-explainer-for-non-geeks-1642909080 [https://perma.cc/3U8S-2BLE] (explaining the "gamergate" movement and its implications).

[9] *See* Tom Downey, *China's Cyperposse*, N.Y. TIMES (Mar. 3, 2010), http://www.nytimes.com/2010/03/07/magazine/07Human-t.html [https://perma.cc/S2GB-JLJQ] (describing instances where the "human flesh search engine" incited Internet users in China).

[10] *Internet Users by Country (2016)*, INTERNET LIVE STATS, http://www.internetlivestats.com/internet-users-by-country/2015/ [https://perma.cc/28FN-GCWJ] (last visited Aug. 24, 2016).

[11] In 2011, the average age of Internet users in China was below thirty years, while in the United States it was thirty-six years. *See* 1 MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY: THE INFORMATION AGE: ECONOMY, SOCIETY, AND CULTURE, 377 (2d ed. 2011). *See also* David Barboza, *China Surpasses U.S. in Numbers of Internet Users*, N.Y. TIMES (Jul. 26, 2008), http://www.nytimes.com/2008/07/26/business/worldbusiness/26internet.html?_r=1 [https://perma.cc/EV23-Q8BN] (describing the population percentage of Internet users in China and their demographic information).

information in the highly regulated traditional media, such as television and newspapers, renders BBS as crucial media outlet for Chinese citizens. Furthermore, the interactive nature of BBS, as well as the large number of BBS users (man-power), make BBS an ideal platform for the human flesh search engine. With the help of BBS, Internet users are able to post and re-post controversial stories, and discuss these stories in a variety of formats including text, image, emoji, audio and video. In many cases, the human flesh search engine can even trigger a chain of media reactions, i.e. traditional media such as television and newspapers following up with reports about the human flesh search engine, thus reinforcing its influence. For instance, the Chinese national television, as well as some mainstream newspapers, reported the Wang Fei case after the event was heavily discussed on the Internet.

Third, compared to concerns over political issues, concerns over ethical issues are more readily raised on the Chinese Internet and are more likely to trigger the human flesh search engine. In the United States, political issues are often at the center of debate on the Internet. By contrast, the majority of online discussion in China raises ethical issues and the ethics and values of family and marriage appear to be most important to Chinese Internet users. As some commentators noted, most Chinese Internet users are much more interested in finding dates, jobs, and entertainment than in engaging in political discourse; online discussion about ethical issues is one significant area that is unfettered by government regulation.[12] In many ways, the human flesh search engine in the Internet age reminds us of the *Da Zi Bao* (Big-character Posters) during the Cultural Revolution of the 1960s and 1970s.[13] In both instances, Chinese people are provoked to participate in mob interaction, conduct mass intimidation, and seek populist revenge against specific individuals. The difference is that the former typically focuses on ethical issues, and the latter on political issues. If political discussion is restricted in Chinese public discourse today, then there must be another outlet

[12] Downey, *supra* note 9.

[13] The Cultural Revolution was launched in May 1966, in which Chinese citizens participated in massive criticisms against bourgeois and corrupt officials. Most criticisms were made through the use of Big-character Posters, which are handwritten, wall-mounted posters using large-sized Chinese characters. *See* THE CHINESE CULTURAL REVOLUTION AS HISTORY (Joseph Esherick et al. eds., 2006); ANDREW WALDER. CHINA UNDER MAO: A REVOLUTION DERAILED (2015).

for civil engagement—that is ethical discussion. The Internet, as illustrated by the human flesh search engine, meets the demand of such ethical discussion.

Fourth, the collectivist culture embedded in Chinese society, as opposed to the individualist culture of the United States, makes Chinese Internet a more suitable ground for the human flesh search engine. Numerous sociological and anthropological studies argue that Chinese culture emphasizes collectivism, whereas American culture emphasizes individualism.[14] The human flesh search engine is a grassroots, collective phenomenon, where Internet users conduct a collaborated search against a person. A collectivist culture like the Chinese is far more likely to trigger collective action. This is also evident when we examine the aggressive actions taken by Chinese Internet users whilst using the human flesh search engine.[15] Moreover, this collectivist-individualist dichotomy can also be applied to the analysis of culpability. As we shall see in the following section, the Wang Fei case demonstrates how culpability is located not just at the level of the individual (Wang Fei), but also at the level of the family unit (his brother, his mother and father), which constitutes a kind of distribution of harassment. This distribution of harassment is less likely to happen in the United States, which focuses more on individual culpability, rather than assigning culpability on a collective level.

Fifth, let us not forget that the level of development of technologies plays a part here. In the United States, because of the advancement of the Internet and related technologies, such as Big Data and the Cloud, the capacities to collect and store personal information has drastically increased by orders of magnitude in the past three decades. Thus, there is simply more digitalized personal information stored on the Internet, gathered either by private companies, such as Google and Apple, or by governmental agencies, such as the FBI and the NSA. With more personal information collected and saved on the Internet, it is much easier for people to cull

---

[14] For studies about individualism and collectivism in different cultures, see GEERT HOFSTEDE, CULTURE'S CONSEQUENCES: INTERNATIONAL DIFFERENCES IN WORK-RELATED VALUES 209–278 (2d ed. 2001); RONALD INGLEHART, MODERNIZATION AND POSTMODERNIZATION: CULTURAL, ECONOMIC AND POLITICAL CHANGE IN 43 SOCIETIES 67–108 (1997).

[15] *See, e.g.*, Downey, *supra* note 9 (denoting several aggressive acts and threats toward targets of the human flesh search engine); *infra* text accompanying note 21.

an information gathering process within the Internet. However, there is still limited personal information collected on the Internet in China. This is partly because the Internet technologies are disproportionally developed across the country,[16] and partly because the majority of middle-age people, who are more likely to be the targets of ethically-related human flesh search engine, do not have a large digital footprint before their thirties. Even if one tries doxing on the Chinese Internet against a middle-age person, the chances of success at obtaining relatively complete personal information are much lower than in the United States.

In sum, although we can readily find some similar Internet phenomenon in other countries, the human flesh search engine is a typical Chinese Internet phenomenon. Among all the Chinese cases involving the human flesh search engine, the Wang Fei case is the first and most important legal case.

B. The Wang Fei Case

On December 29, 2007, Jiang Yan committed suicide in Beijing.[17] Several days later, her diary, which revealed her misery after discovering her husband Wang Fei's adultery, was posted and distributed online by Zhang Leyi.[18] Soon after that, Chinese Internet users launched the human flesh search engine to locate the cheating husband.[19] The posts and reposts of this affair elicited thousands of responses on several BBS in the following few days, and Wang Fei soon found himself at the top of a "most wanted" list on the Chinese Internet.[20] The angry Internet users sniffed out and posted his photos, home and work addresses, phone numbers, student identity number,

---

[16] This is the "digital divide", which refers to the differences between those who have access to, use of, or impact on the Internet and those who do not have such privileges. Generally speaking, the digital divide is more evident in developing countries. *See* Michelle W. L. Fong, *Digital Divide: The Case of Developing Countries*, 6 ISSUES IN INFORMING SCI. INFO. TECH. 471, 476 (2009).

[17] *Renrou Sousuo Diyi An* (人肉搜索第一案) [*The First Human Flesh Search Engine Case*], BAIDU BAIKE (百度百科), http://baike.baidu.com/view/3107502.htm [https://perma.cc/8EVW-PLRV].

[18] *Id.*

[19] *Id.*

[20] *Id.*

national identity number, and even his brother's license-plate number on major online portals.[21] Two of these online portals stood out.

The first online portal was tianya.cn ("Tianya"), a leading and most widely read Chinese BBS, which, at the time, had approximately 11 million weekly visits. Much of the information transmitted over Tianya originates with the website's millions of registered users. In early January of 2008, Wang Fei's name was first revealed in an online post in Tianya, and other personal information of him and his mistress was disclosed shortly after.[22] One early comment by an anonymous user read, "We should take revenge on that couple and drown them in our sputa".[23] Another Internet user called for mob justice: "Those in Beijing, please share with others the scandal of these two. Make it impossible for them to stay in this city".[24] Vulgar insults like "F*** your mother"[25], "D*** your family"[26] and "You are the murder[er]"[27] were directed towards Wang Fei, his mistress, and his family.[28] Wang Fei then filed a complaint letter to Tianya, requesting the website to take down online posts containing his personal information. On March 23, 2008, almost three months after the initial publication of Wang Fei's personal information, Tianya finally took down these content.

The other forum was daqi.com ("Daqi"). Originally known as ChinaBBS, Daqi was one of the earliest online forums on the Chinese Internet. Daqi created their own news reports and comments about current events. It also hosts a number of interactive features

---

[21] *Id.* Some of this information is still publicly available. *See Beijing Jiang Yan Wang Fei Dongfang Enna Zhaopian Boke MSN Kongjian* (北京姜岩王菲东方恩纳照片博客 MSN 空间) [*Photos, Blogs and MSN Spaces of Jiang Yan, Wang Fei, and Dongfang Enna in Beijing*] XINLANG LUNTAN (新浪论坛) (Jan. 15, 2008), http://club.history.sina.com.cn/thread-2624045-1-1.html [https://perma.cc/2RTW-JKSB].

[22] *Beijing Cong 24 Lou Tiaoxi Zisha de MM Zuihou de Riji* (北京从 24 楼跳下自杀的 MM 最后的日记) [*The Last Dairy of a Girl Who Committed Suicide from the Twenty-Fourth Floor in Beijing*], TIANYA ZATAN (天涯杂谈) (Jan. 10, 2008), http://bbs.tianya.cn/post-free-1094240-1.shtml [https://perma.cc/P97Z-4BTL].

[23] Downey, *supra* note 9.

[24] Downey, *supra* note 9.

[25] TIANYA ZATAN, *supra* note 22.

[26] TIANYA ZATAN, *supra* note 22.

[27] TIANYA ZATAN, *supra* note 22.

[28] Chen Wanying, *Will the First "Human Flesh Search" Trial Set Restrictions on the Practice?*, EAST SOUTH WEST NORTH (東南西北) (July 31, 2008), http://zonaeuropa.com/20080802_1.htm [https://perma.cc/9PDT-UDMS] (summarizing the first "human flesh search" case regarding Wang Fei as a target of Internet users in China for alleged infidelity to his wife).

that allow Internet users to respond to the editors and commentators by posting their own thoughts and ideas. Soon after the public discussion raised by Jiang Yang's suicide, Daqi timely created a theme web page entitled "The last blog by a suicide girl who jumped from the 24th floor". The theme web page cited Wang Fei's personal information as well as nefarious comments and provided a brief on Jiang Yan's suicide, hyperlinks to related online content, a summary of online criticism, analysis by a psychology expert, and interviews with relevant individuals (Zhang Leyi, a classmate of her sister, and her lawyer). As a result, many Internet users went to Daqi in order to criticize and threaten Wang Fei and his mistress.

Wang Fei and his family were also harassed and threatened in the real world. Not long after his cell phone number was published, Wang Fei received a high volume of offensive and threatening phone calls and text messages. Some even included death threats. Wang Fei had to move to his parents' house to escape angry Internet users. Expletives were spray-painted on the doors of his parents' house, including words like "whoever sheds man's blood, by man his blood shall be shed" and "you killed a good wife."[29] Strangers also contacted Wang Fei's company, a multinational advertising agency, which later fired him and his mistress. He was afraid to leave his house, and was not able to find a decent new job for almost two years. As Wang Fei himself put it, "the human flesh search engine completely ruined my personal life."[30]

In March 2008, Wang Fei brought lawsuits against Zhang Leyi, Tianya, and Daqi in Beijing Chaoyang District Court, which marked the most important case by far concerning the human flesh search engine in China. The Beijing Chaoyang District Court made three decisions (one for each defendant) on December 18 of that same year.

In the decision for Zhang Leyi, the Beijing Chaoyang District Court held that the defendant was liable for infringing on Wang Fei's right to privacy and his right to reputation. Beijing Chaoyang District Court found that through his website and blog, Zhang Leyi unlawfully publicized the affairs of Wang Fei and his mistress, as

[29] *Id.*
[30] *Id.*

well as Wang Fei's personal information.[31] According to the decision, privacy includes private life, private information, private space and personal seclusion.[32] The Beijing Chaoyang District Court defined the right to privacy as a type of right of personality, which provides individuals control over their secrecy and their personal lives, and protects them from intervention by others.[33] The Beijing Chaoyang District Court maintained that not only was personal identifiable information subject to privacy-related restrictions, but so too was the affair itself.[34] Therefore, it concluded that publicizing this information violated Wang Fei's right to privacy as well as his right to reputation. The legal basis for this decision was predicated mainly on article 101 of General Principles of the Civil Law, which provides protection to individuals' personal dignity and reputation.[35] Zhang Leyi was required to remove all infringing content on his website (including three blog articles and a photo of Wang Fei and his mistress), to make public apology on the front-page of his website, and to pay damages for emotional distress of RMB 5,000 to Wang Fei.[36]

In the decision for the second defendant, Daqi, the Beijing Chaoyang District Court recognized the fact that soon after the public concern raised by Jiang Yang's suicide, the website created the theme page of this incident, and allowed Internet users to comment on related topics on their BBS.[37] The Beijing Chaoyang District Court held that in building the theme web page, conducting investigations and interviews, and cross-referencing other websites, Daqi expanded the event's influence and helped distribute Wang Fei's private

---

[31] Wang Fei Su Zhang Leyi (王菲诉张乐奕) [Wang Fei v. Zhang Leyi], 2008 CHAOMIN CHUZI 10930 (Beijing Chaoyang Dist. People's Ct. Dec. 18, 2008), http://www.chinacourt.org/article/detail/2008/12/id/337282.shtml [https://perma.cc/483S-T9UJ].

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] Article 101 of General Principles of the Civil Law states that: "[C]itizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited." Minfa Tongze (民法通则) [General Principles of Civil Law] (promulgated by the Nat'l People's Cong., Apr. 12, 1986, effective Jan. 1, 1987), art. 101.

[36] Wang Fei Su Zhang Leyi, s*upra* note 31.

[37] Wang Fei Su Daqi Wang (王菲诉大旗网) [Wang Fei v. Daqi.com], 2008 CHAOMIN CHUZI 29276 (Beijing Chaoyang Dist. People's Ct. Dec. 18, 2008), http://www.chinacourt.org/article/detail/2008/12/id/337278.shtml [https://perma.cc/6VXC-TSDZ].

information among the general public.[38] After the publication of the theme web page, many internet users continued to spread the information and criticized Wang Fei in Daqi on other online forums.[39] Later, these online criticisms turned to personal threats, bullying and stalking in the real world, which became so intensive and protracted that they seriously affected Wang Fei's life and damaged his social reputation.[40]

In its decision, the Beijing Chaoyang District Court invoked two administrative regulations that were stipulated to establish the liability of Internet service providers: the Regulation on Internet Information Service and Management Provisions on Electronic Bulletin Services in Internet.[41] These regulations provide that the Internet service providers shall provide reliable services to Internet users and guarantee the legality of the content.[42] Specifically, no one may publish information that might insult or slander or infringe upon the lawful rights of others in the electronic bulletin board service system.[43] In cases where an Internet service provider finds such

---

[38] *Id.*

[39] *Id.* In previous cases, the Beijing Chaoyang District Court has also held a website liable for publishing defamatory reports and articles. *See, e.g.*, Gao Xiaosong Su Yahu Xianggang Konggu Youxian Gongsi (高晓松诉雅虎香港控股有限公司) [Gao Xiaosong v. Yahoo! (Holdings) Hong Kong Ltd.], 2002 CHAOMIN CHUZI 04336 (Beijing Chaoyang Dist. People's Ct. Dec. 19, 2003), http://www.cnipr.net/article_show.asp?article_id=8621 [https://perma.cc/N5T2-YY9D].

[40] *Id.*

[41] *Id.*

[42] Article 13 of Measures for the Administration of Internet Information Services provides that "[A]n Internet information services provider shall provide good quality services to Internet users and shall ensure the legality of the information provided by it." Hulianwang Xinxi Fuwu Guanli Banfa (互联网信息管理办法) [Measures for the Administration of Internet Information Services] (promulgated by the State Council, Sept. 25, 2000, effective Sept. 25, 2000), art. 13, *translated in Administrative Measures on Internet Information Services*, CHINA.ORG.CN, http://www.china.org.cn/business/2010-01/20/content_19274704.htm [https://perma.cc/DJ87-3EZE].

[43] Article 15 section 8 of Measures for the Administration of Internet Information Services provides that "[I]nternet information service providers may not produce, reproduce, disseminate or broadcast information with content that insults or slanders a third party or infringes upon the lawful rights and interests of a third party." Hulianwang Xinxi Fuwu Guanli Banfa, *supra* note 42. Article 9 section 8 of the Management Provisions on Electronic Bulletin Services in Internet provides that "[N]o one may publish information in an electronic messaging service system with content that insults or slanders a third party or infringes upon the lawful rights and interests of a third party." Hulianwang Dianzi Gonggao Fuwu Guanli Guiding (互联网电子公告服务管理规定) [Management Provisions on Electronic Bulletin Services] (promulgated by the Ministry of Industry and Information Technology, Nov. 6, 2000, effective Nov. 6, 2000), art. 9.

information, the Internet service provider must delete it promptly, preserve related records and report them to relevant state authorities.[44] Daqi did not fulfill its obligation as an Internet service provider in China. Therefore, the Beijing Chaoyang District Court held that Daqi violated Wang Fei's right to privacy and his right to reputation.[45] Daqi was required to remove the related theme web page, to make public apology on the front-page of its website, and to pay damages for emotional distress of RMB3,000 to Wang Fei.[46]

Beijing Chaoyang District Court took a relatively balanced approach in the decision for Tianya. It affirmed the facts that the Internet was developing rapidly in China, and that the number of Internet users had exceeded 200 million at the time of the Wang Fei case, thus surpassing traditional media to become the largest media outlet.[47] The court also held that due to the diversity of Chinese characters and the continuous change in online language, it would be truly impossible for Chinese internet service providers to comb through all messages and monitor every online post before publication.[48] Therefore, with respect to monitoring online posts, the liability for Internet service providers should be limited to their knowledge of the legality of the content. Internet service providers that knowingly allow the existence and spread of illegal or infringing information shall be held accountable under contributory infringement.[49] Internet service providers shall not be held accountable if they take down illegal content in a timely manner.[50]

---

[44] Article 16 of Measures for the Administration of Internet Information Services provides that "[I]f an Internet information service provider discovers that information transmitted by its website clearly falls within the contents listed in Article 15 hereof, it shall immediately discontinue the transmission of such information, keep relevant records and make a report to relevant State authorities." Hulianwang Xinxi Fuwu Guanli Banfa, *supra* note 42. Article 13 of the Management Provisions on Electronic Bulletin Services in Internet provides that "[I]f an electronic messaging service provider discovers that information transmitted by its service system clearly falls within the contents listed in Article 9 hereof, it shall immediately delete such information, keep relevant records and make a report to relevant State authorities." Hulianwang Dianzi Gonggao Fuwu Guanli Guiding, *supra* note 43, art. 13.

[45] Wang Fei Su Daqi Wang, s*upra* note 37.

[46] Wang Fei Su Daqi Wang, s*upra* note 37.

[47] Wang Fei Su Tianya (王菲诉天涯) [Wang Fei v. Tianya], 2008 CHAOMIN CHUZI 29277 (Beijing Chaoyang Dist. People's Ct. Dec. 18, 2008), http://www.chinacourt.org/article/detail/2008/12/id/337281.shtml [https://perma.cc/Y43E-TTFZ] (last visited May 24, 2016).

[48] *Id.*

[49] *Id.*

[50] *Id.*

In this case, Tianya took down, in due course, the alleged infringing information after receiving complaints from Wang Fei.[51] Thus, Beijing Chaoyang District Court held that Tianya was not liable.[52]

In sum, based on article 15 section 8 of the Regulation on Internet Information Service,[53] article 9 section 8 of the Management Provisions on Electronic Bulletin Services in Internet,[54] and article 101 of General Principles of the Civil Law,[55] Zhang Leyi and Daqi were held liable for infringing Wang Fei's right to privacy and the right to reputation. Tianya, on the other hand, had fulfilled its notice-take-down obligation, and thus was not held liable. Zhang Leyi appealed the decision in early 2009 and the upper level court, the Beijing No. 2 Intermediate Court, affirmed the decision on December 23, 2009.[56]

III. BALANCING PRIVACY AND FREE SPEECH

The human flesh search engine expands the significance of the tension between privacy and free speech, and brings to light new perspectives on the balance between them.[57] By focusing on U.S. constitutional analysis, this section will open up the discussion about balancing privacy and free speech in the digital age.

The First Amendment, on its face, prohibits any effort of the government to abridge "the freedom of speech, or of the press."[58] However, as Justice Holmes' famous aphorism about the right to shout 'fire' in a crowded theater when there is no fire, the First

---

[51] *Id.*

[52] *Id.*

[53] Hulianwang Xinxi Fuwu Guanli Banfa, *supra* note 42.

[54] Hulianwang Dianzi Gonggao Fuwu Guanli Guiding, *supra* note 43.

[55] Article 101 of General Principles of the Civil Law provides that "citizens and legal persons shall enjoy the right of reputation. The personality of citizens shall be protected by law, and the use of insults, libel or other means to damage the reputation of citizens or legal persons shall be prohibited." Minfa Tongze, *supra* note 35, art. 101.

[56] Wang Fei Su Zhang Leyi (王菲诉张乐奕) [Wang Fei v. Zhang Leyi], 2009 ERZHONGMIN ZHONGZI 5603 (Beijing No. 2 Interm. People's Ct. Dec. 23, 2009), http://www.pkulaw.cn/case/payz_117802834.html [https://perma.cc/7GBZ-F3HK].

[57] Although physical violence associated with the human flesh search engine is conduct rather than speech, the creation and dissemination of personal information on the Internet can be considered as speech for the First Amendment purposes. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 527 (2001) (regulating disclosures on the internet is considered a regulation of speech).

[58] This view was famously held by Justice Hugo Black, who asserted that "no law" means no law. *See* Konigsberg v. State Bar of Cal., 366 U.S. 36, 61–63 (1961) (Black, J., dissenting) (stating "the commands of the First Amendment are stated in unqualified terms").

Amendment right is not absolute.[59] When in conflict with other interests such as the right to privacy, restrictions on speech historically have been considered justifiable. Thus, the human flesh search engine poses an instance that requires careful analysis of the balance between privacy and free speech.[60]

According to Alexander Meiklejohn, the key purpose of speech protection is to preserve the open debate that is necessary for the health of democracy.[61] In light of this, the First Amendment is most concerned with political speech because of its importance to democratic deliberation and self-government. Indeed, compared to other kinds of speech,[62] the U.S. Supreme Court has set the highest threshold for restrictions on political speech.[63] Meanwhile, the U.S. Supreme Court's protection of speech for private individuals and of private concern is comparatively not as stringent. Most of the online speech in the Wang Fei case is speech about private individuals and of private concern. The question then is: do restrictions on this kind of speech violate the First Amendment?

To answer this question, we might first turn to the analytical framework that the U.S. Supreme Court has used in relevant First Amendment cases. The first step of the analysis is to decide whether the challenged law is content-based or content-neutral.[64] If the

---

[59] Schenck v. U.S., 249 U.S. 47, 52 (1919).

[60] *See* Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L. J. 943, 945 (1987) (explaining more about balancing values on constitutional questions).

[61] ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT, IN POLITICAL FREEDOM: THE CONSTITUTIONAL POWERS OF THE PEOPLE 3 (1960) (originally published 1948).

[62] Traditionally, the First Amendment imposes tight constraints upon government efforts to restrict political speech, while imposing looser constraints when the government seeks to restrict commercial speech. *See, e.g.*, Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 562, 563 (1980) (stating the Constitution provides lesser protection to commercial speech).

[63] These higher standards relied on the "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open," New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964); s*ee also* Terminiello v. Chicago, 337 U.S. 1, 4 (1949) (stating that the vitality of civil and political institutions depends on free discussion); De Jonge v. Oregon, 299 U.S. 353, 365 (1937) (concluding that free political discussion is imperative in part because it ensures the government is more responsive to the "will of the people" and promotes change through peaceful means); Whitney v. Cal., 274 U.S. 357, 375–76 (1927) (Brandeis, J., concurring) (stating that the Founders believed freedom of speech was indispensable to the discovery and spread of political truth).

[64] "As a general rule, laws that by their terms distinguish favored speech from disfavored speech on the basis of the ideas or views expressed are content based." Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 643 (1994).

challenged law is found to be content-neutral, the Court generally applies "intermediate scrutiny" and balances relative social costs and benefits.[65] If the challenged law is content-based, it is "presumptively invalid" and the Court will apply strict scrutiny.[66] Insofar as the government forbids communicating private information about other persons, the restriction is clearly directed at the content of the communication. Therefore, the content-neutral analysis is almost irrelevant to the analysis of the human flesh search engine.

As a result, the U.S. Supreme Court would have needed to apply strict scrutiny to decide whether content-based restrictions on free speech in the Wang Fei case could have been permitted.[67] Content-based speech restrictions are generally unconstitutional unless they are narrowly tailored to a compelling state interest—the two-prong test that the U.S. Supreme Court usually applies.[68] Historically, content-based restrictions on free speech have been permitted for incitement, obscenity,[69] defamation,[70] speech integral to criminal conduct,[71] fighting words,[72] child pornography,[73] fraud,[74]

---

[65] *See, e.g.*, Hill v. Colo., 530 U.S. 703, 723, 724 (2000) (holding that when a content-neutral regulation does not entirely foreclose any means of communication, it may satisfy the standard of scrutiny even though it is not the least restrictive means of serving the statute's goal).

[66] *See, e.g.*, U.S. v. Playboy Ent. Grp., Inc., 529 U.S. 803, 813 (2000) ("[A] content-based speech restriction . . . can stand only if it satisfies strict scrutiny.").

[67] *Id.*

[68] Turner Broadcasting System, Inc. v. F.C.C., 512 U.S. 622, 680 (1994).

[69] *See, e.g.*, Miller v. Cal., 413 U.S. 15 (1973) (holding that obscene material is unprotected by the First Amendment).

[70] *See, e.g.*, Gertz v. Robert Welch, Inc., 418 U.S. 323, 346 (1974) (concluding that notwithstanding the First Amendment, States should retain substantial latitude to enforce legal remedies for defamatory falsehoods).

[71] *See, e.g.*, Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 496 (1949) (holding that Missouri statute prohibiting collusive agreements in restraint of trade do not violate constitutional guarantees of freedom of speech).

[72] *See, e.g.*, Chaplinsky v. N.H., 315 U.S. 568, 572 (1942) (holding that "fighting words" are not in any proper sense communication of information or opinions safeguarded by the Constitution).

[73] *See, e.g.*, New York. v. Ferber, 458 U.S. 747, 764 (1982) (holding that child pornography is not entitled to First Amendment protection).

[74] *See, e.g.*, Virginia State Pharmacy Board v. Virginia Citizens Consumer Council, 425 U.S. 748, 771 (1976) (stating that "untruthful speech, commercial or otherwise, has never been protected for its own sake").

true threats,[75] and speech presenting some grave and imminent threats.[76] According to these precedents, true threats and fighting words in the Wang Fei case, both on and off the Internet, deserve no First Amendment protection. But what about the aggregation and publication of Wang Fei's personal identifiable information (such as his cellphone number, home address, photos, and national identity number) on the Internet? In other words, could restrictions on speech about private individuals, if narrowly tailored, satisfy the compelling interest prong of First Amendment strict scrutiny? This Note argues that certain restrictions on this type of speech are justifiable in the Internet age.

A. Privacy in the Digital Age

As if past social and technological changes were not enough to cause concern to the right to privacy, almost a century after the publication of Warren and Brandies' article[77] the Internet arrived. The advances of the Internet and related technologies, such as Big Data and the Cloud, have caused a larger disruption than any previous technology and they have specifically sparked debate around information privacy.[78]

So how has this disturbance manifested? First, many fragments of personal information collected by new technologies, saved in databases and scattered across the Internet. Once digitized, it is difficult to control their circulation and dissemination on the Internet. Even those who have never used the Internet are likely to have some personal information online.[79] As Yochai Benkler notes,

---

[75] *See, e.g.*, Watts v. U.S., 394 U.S. 705, 707-08 (1969) (holding the U.S. has a valid interest in protecting the President's safety and may prohibit threats against the President where the government proves they were "true" threats).

[76] *See, e.g.*, Near v. Minn., 283 U.S. 697, 706 (1931) (holding that a publication that maliciously defames and bullies people was considered a public nuisance).

[77] *See generally* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, (1890). It is also worth noting that Brandeis also wrote some of the greatest prose for free speech, such as his concurring opinion in Whitney v. California, 274 U.S. 357, 372 (1927).

[78] For example, photography, audio, and video recording technologies did bring concerns over the control of personal information, but not as much as Internet technology.

[79] A homeless beggar in the city of Ningbo, Brother Sharp, was a target of human flesh search engine after an amateur photographer posted pictures of him walking the streets onto the Chinese Internet. Clifford Coonan, *Handsome Chinese Vagrant Draws Fans of 'Homeless Chic'*, INDEPENDENT (Mar. 3, 2010), http://www.independent.co.uk/news/world/asia/handsome-chinese-vagrant-draws-fans-of-homeless-chic-1915812.html

many of the problems spawned by the Internet are due to the "destabilization" of traditional information flows in everyday life.[80] The power of controlling personal information has been continually transferred from individuals to Internet intermediaries. The underlying assumption of previous privacy-related legal doctrines is that individuals who are concerned about their personal information will undertake reasonable, though imperfect, actions to protect their privacy by controlling how, when, where, and to whom they reveal their personal information. This assumption has been challenged by these new Internet technologies, and legal doctrines that rely on it should be adjusted accordingly.

Second, personal information that used to be "scattered, perishable and localized is becoming searchable, permanent and widespread". [81] Companies, particularly Internet intermediaries, archive digitalized personal information and ensure the longevity of such information, which stand to follow individuals in perpetuity. Moreover, Google and other search engines provide efficient ways to locate personal information of individuals. For example, in the past, Wang Fei's personal information would have been gradually forgotten, and he might at least have an option to move to a new place and start a new life. This is impossible in the digital age today. Not only can the Internet and other technologies allow people to obtain his personal information to see, but they can also continue to make his personal information almost permanently available online. Indeed, these technological developments have underscored the concerns about the balance between privacy and free speech.

B. Speech: Moving from the Offline World to the Online World

Previous doctrines of free speech are being challenged by the development of the Internet and related technologies.[82] First, the

---

[https://perma.cc/K8QP-2QHC]. The case of Andrew Fledmar described by Mayer-Schönberger presents similar concerns. *See* VICTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 3–5 (2009).

[80] Yochai Benkler, *Net Regulation, Taking Stock and Looking Forward*, 71 U. COLO. L. REV. 1203, 1238–40 (2000).

[81] DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 4 (2007).

[82] For discussion about the First Amendment issues in the early days of Internet age, *see generally* Owen Fiss, *In Search of a New Paradigm*, 104 YALE L.J. 1613 (1995); Cass R. Sunstein, *The First Amendment in Cyberspace*, 104 YALE L.J. 1757 (1995); Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743 (1995).

Internet is a public forum that allows numerous Internet users to function as a crowd, which acts in unison to criticize one or more individuals. Over a century ago, Gustave Le Bon suggested that individuals in a crowd assimilate easily, develop a herd mentality, and lose their individual personalities.[83] This is the social phenomenon we witness in the human flesh search engine, where individuals falsify their own knowledge, or at least suppress their own doubts, in the face of the apparent views of a crowd. Most public humiliation and defamation speech in the human flesh search engine reflect Internet users' strong opinions and little actual or first-hand knowledge regarding the given debate. As the volubility of opinion grows, so too do the number of Internet users who subscribe to that opinion, irrespective of whether it is actually true in a factual sense. Internet-based group-thinking of this sort exacerbates unjustified critique, creates and propagates falsehoods, and potentially damages the reputation of individuals.

Secondly, as Cass Sunstein rightly points out, through social cascades and group polarization, online speech is very likely to "go extreme."[84] And extreme deliberation makes the crowd far more likely to support aggressive protest actions. In the Wang Fei case, public humiliation and defamation speech pervaded the human flesh search engine, creating a hostile environment that discouraged reasonable conversation. At that time, no one cared about the facts that Wang Fei and his wife were separated, and that Wang Fei's wife had suffered mental illness for quite a long time. Furthermore, when the public humiliation reached a tipping point, some Internet users eventually took aggressive actions to intervene in Wang Fei's life.

Thirdly, Internet users can easily exploit the anonymity of the Internet to target helpless victims with vile speech that invades privacy, ruins reputations, or spreads prejudice. As Daniel Solove points out, "when people are less accountable for their conduct, they are more likely to engage in unsavory acts."[85] With the speakers being anonymous, online speech is "often much nastier and more

---

[83] GUSTAVE LE BON, THE CROWD: A STUDY OF THE POPULAR MIND 7–43 (1896).

[84] CASS R SUNSTEIN, GOING TO EXTREMES: HOW LIKE MINDS UNITE AND DIVIDE 1–5, 21–37 (2009). Social cascade occurs when a group of early movers say or do something and other people follow their signal because individuals tend to rely on what other people think and do. Group polarization refers to the fact that when likeminded people get together, they often end up thinking a more extreme version of what they thought before they started to talk to one another.

[85] Solove, *supra* note 81, at 140.

uncivil," and "it is easier to say harmful things about others when we don't have to take responsibility."[86] Moreover, Yochai Benkler argues that the Internet eliminated the intermediaries that were gatekeepers to control the dissemination of, and access to, speech.[87] With the Internet, almost anything that anyone was willing to put online was available directly to anyone else.[88] Last but not least, without personal experience, it is particularly difficult to become well-informed about a person through the Internet. Individuals will be "judged, fairly or unfairly, on the basis of isolated bits of personal information that are taken out of context."[89] Therefore, a single negative revelation or fabrication proliferated online could ruin one's reputation beyond the possibility of redress.[90] In the Wang Fei case, the Internet will always remember Wang Fei as a terrible husband whose adultery caused his wife to commit suicide. Indeed, in many cases of the human flesh search engine, these perceptions might well become a constituent part of the victims' identity, where they have to bear these stigmas for the rest of their lives.

Because of these characteristics of online speech, the Brandenburg test that U.S. Supreme Court heavily relied on in the past few decades—whether the speech is "directed to inciting or producing imminent lawless action and is not likely to incite or produce such action"[91]—should be reconsidered in the Internet age. The author contends that because of the increased danger of online speech towards private individuals, the Brandenburg test is no longer adequate for the analysis.

In *Cohen v. California*, while judging a man for wearing a jacket bearing the words "Fuck the Draft" inside the Los Angeles Courthouse, the Court overturned his conviction for disturbing the peace.[92] In that case, the Court did not believe that "substantial numbers of citizens are standing ready to strike out physically at

---

[86] *Id*.

[87] Benkler, *supra* note 80, at 1203.

[88] *Id*.

[89] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 200 (2000).

[90] SAUL LEVMORE & MARTHA NUSSBAUM, THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 1–3 (2010).

[91] Brandenburg v. Ohio, 395 U.S. 444, 447 (1969).

[92] Cohen v. Cal., 403 U.S. 15, 26 (1971).

whoever may assault their sensibilities with execrations like that uttered by Cohen."[93]

But the Wang Fei case is different. Posting personal information online is not delivering a handbill or a pamphlet in a courthouse. A significant number of Internet users were incited by the online speech to take lawless actions with enduring effect on Wang Fei and his family. In *United States v. Dinwiddie*, Judge Arnold explained that the alleged threat must be analyzed in light of its entire factual context to determine whether the recipient of the alleged threat could reasonably conclude that it expresses a determination or intent to injure presently or in the future.[94] In the Wang Fei case, Internet users not only posted vicious statements—such as "whoever sheds man's blood, by man his blood shall be shed" and "you killed a good wife"— but also spray-printed them on the door of Wang Fei's home using the information provided by the human flesh search engine. In this context, a reasonable person would foresee that a combination of those vicious statements and the publication of Wang Fei's personal information "would be interpreted by those to whom the maker communicates the statement as a serious expression of intent to harm and assault."[95] Both the Internet users and Internet intermediaries understood the purpose of distributing Wang Fei's personal information: to expose him to public humiliation and harassment. Therefore, such online speech should be assigned less weight when balanced against privacy protections.

C. Speech about Private Individuals and of Private Concern vis-a-vis Speech about Public Officials and of Public Concern

Here, the distinction between private individuals and public officials, and between public and private concern, are crucial for a more nuanced understanding of online speech protection. When regulating distressing or outrageous speech, the U.S. Supreme Court looks at whether speech is of private or public concern to determine

---

[93] *Id.* at 23.

[94] U.S. v. Dinwiddie, 76 F.3d 913, 925 (8th Cir. 1996).

[95] Planned Parenthood v. Am. Coalition of Life Activists, 290 F.3d 1058, 1074 (9th Cir. 2002) (holding that the posters constituted a true threat. The court reasoned that in three prior incidents, a "wanted"-type poster identifying a specific doctor who provided abortion services was circulated, and the doctor named on the poster was killed. The activists and physicians knew of this, and both understood the significance of the particular posters specifically identifying each of them).

the appropriate level of First Amendment protection.[96] As Justice Roberts points out in *Snyder v. Phelps*, "not all speech is of equal First Amendment importance, however, and where matters of purely private significance are at issue, First Amendment protections are often less rigorous."[97]

Moreover, as Daniel Solove argues, under theories that support free speech—democratic self-governance, the market-place of ideas, and individual autonomy [98] —speech about private individuals and of private concern "does not strongly further the interests justifying free speech."[99]

Finally, the Internet has occasioned the proliferation of online speech about the private concern of private individuals. This type of speech is potentially much more harmful to information privacy than other types of online speech. The vast majority of online speech has little to do with issues of public concern, but it has a lot to do with private concerns of individuals' lives.[100] Therefore, restrictions on such speech might well be more justifiable.[101]

The distinctions between private individuals and public officials and between public and private concern are not novel in the U.S. Supreme Court's prior decisions. In *Bartnicki v. Vopper*, the Court held, by a vote of 6-3, that the government could not constitutionally punish the media for broadcasting an unlawfully wiretapped telephone conversation where the information was related to both public officials and public concern.[102]

---

[96] Dun & Bradstreet, Inc. v. Greenmoss Builders, 472 U.S. 749, 758–59 (1985).

[97] Snyder v. Phelps, 562 U.S. 443, 452 (2011).

[98] However, affirmative claims of free speech cannot be easily dismissed. These are the three most important theories for free speech, all of which require refinement for their applications in the Internet age.

[99] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 986–1000 (2003). For the three theories addressing the scope of First Amendment speech protection, see C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. REV. 964, 990–1009 (1978) (describing these methods and concluding constitutional protection of speech is justified because freedom of speech is for nonviolent and "noncoercive" speech).

[100] Jack M. Balkin, DIGITAL SPEECH AND DEMOCRATIC CULTURE: A THEORY OF FREEDOM OF EXPRESSION FOR THE INFORMATION SOCIETY, 79 N.Y.U. L. REV. 1, 12 (2004).

[101] Solove, *supra* note 99, at 967, 975 (2003) ("[S]peech of private concern is less valuable than speech of public concern and should be assigned less weight.").

[102] The Bartnicki Court held that intermediaries cannot be sanctioned for publishing information of public concerns though it was illegally obtained. Bartnicki v. Vopper, 532 U.S. 514, 528 (2001). The First Amendment reflects "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open." New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964). "[S]peech on 'matters of public

However, the Court left open the question of whether the government could punish commentators or intermediaries if the broadcast had involved only matters related to private individuals and private concern. Traditionally, speech about public officials, as well as celebrities,[103] is protected by the First Amendment unless 'actual malice' is shown.[104] By contrast, speech about private individuals is less strongly protected by the Court,[105] because "there is no threat to the free and robust debate of public issues; there is no potential interference with a meaningful dialogue of ideas," and the "threat of liability" does not pose the risk of "a reaction of self-censorship" on matters of public import.[106]

Deciding whether speech is of public or private concern requires us to examine the "content, form, and context" of that speech.[107] In *Snyder v. Phelps*, the Court wrote: "While these messages may fall short of refined social or political commentary, the issues they highlight—the political and moral conduct of the United States and its citizens, the fate of our Nation, homosexuality in the military, and scandals involving the Catholic clergy—are matters of public import."[108] Borrowing the Court's logic, some might argue that the online commentaries on Wang Fei's adulterous behavior constitute speech of public concern. Such online critiques certainly convey Internet users' positions on this issue, in a manner designed, unlike the private speech in *Dun & Bradstreet,* to reach as broad a public audience as possible via the Internet.

---

concern' . . . is 'at the heart of the First Amendment's protection.'" Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758–759 (1985) (opinion of Justice Powell) (quoting First Nat. Bank of Boston v. Bellotti, 435 U.S. 765, 776 (1978)).

[103] *See generally* Hustler Magazine, Inc. v. Fallwell, 485 U.S. 46 (1988).

[104] New York Times Co. v. Sullivan, 376 U.S. 254, 279, 280 (1964).

[105] The Republicanism argument on free speech protection focuses primarily on the virtue of democratic deliberation and this mostly refers to speech about public officials and of public concern rather than speech of private individuals and of private concern. For instance, in *Stromberg v. California*, the Court held that "the maintenance of the opportunity for free political discussion to the end that government may be responsive to the will of the people and that changes may be obtained by lawful means, an opportunity essential to the security of the Republic, is a fundamental principle of our constitutional system." Stromberg v. California, 283 U.S. 359, 369 (1931). *See also* MEIKLEJOHN, *supra* note 61, at 3.

[106] Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 760. *See also* Toffoloni v. LFB Publ'g Group, 572 F.3d 1201 (11th Cir. Ga. 2009) (stating that under Georgia law, to properly balance freedom of the press against the right of privacy, every private fact disclosed in an otherwise truthful, newsworthy publication must have some substantial relevance to a matter of legitimate public interest).

[107] *Snyder*, 562 U.S. at 444.

[108] *Snyder*, 562 U.S. at 454.

However, there are several reasons that support the private-concern aspect of such speech and the protection of privacy in the Wang Fei case. First of all, online critiques against adultery do not necessarily require knowledge of Wang Fei's personal information, such as his cellphone number, home address, or national identity number, which were generated through the human flesh search engine. Even if some of his personal information—for instance, his relationship with his mistress—could be viewed as contributing to a discussion on a matter of public concern, that would not change the fact that the dominant theme of the human flesh search engine alluded to personal information that had little to do with public concern. Second, the context of the Wang Fei case has shown an intent to disturb, harass, and threaten, even if the speech occurred through a public forum—the Internet. The fact that Internet users spoke in those BBS cannot by itself transform the nature of their speech.[109] Finally, some of the online critiques captured in the Wang Fei case—such as "F*** your mother", "D*** your family" and "You are the murder[er]"—can be considered true threats because they are invitations of hostility, and "like Ryder trucks or burning crosses, they connote something they do not literally say, yet both the actor and the recipient get the message."[110] Although some offensive speech is protected by the First Amendment, it does not protect true threats.[111] Such speech, which relates to cyberstalking,[112] cyberharassment, and cyberbullying, focuses on intimidating, distressing and threatening Wang Fei and his family; it has very little to do with the original policy goals of First Amendment's speech

[109] In a concurring opinion in *Times v. Hill*, Justice Douglas held that when individuals are then in the public domain, such privacy as a person has ceased. This standard could hardly be applied in the Internet age, for one can very easily enter in the public domain (for example, in public discussion of online forums) even he is involuntary. *See* Time, Inc. v. Hill, 385 U.S. 374, 401 (1967) (Douglass, J., concurring).

[110] Planned Parenthood v. American Coalition of Life Activists, 290 F.3d 1058, 1085 (9th Cir. 2002).

[111] Virginia v. Black, 538 U.S. 343, 359–60 (2003).

[112] In the United States, courts often invoke the cyberstalking statute (18 U.S.C. § 2261A(2) (2006)) to regulate cyberstalking. *See, e.g.*, United States v. Bowker, 372 F.3d 365, 371–72 (6th Cir. 2004) (holding that the defendant liable for disturbing emails and letters, making phone calls to his victim over the course of about a year, and following his victim to West Virginia and engaged in vaguely threatening behavior.); United States v. Shrader, No. 1:09-CR-00270, 2010 U.S. Dist. LEXIS 10820, at *5 (S.D. W. Va. Feb. 8, 2010) (holding the defendant liable for calling his ex-girlfriend daily for about two months and sending her a thirty-two-page letter saying she had two weeks to decide what to do before he initiated his next step).

protection, i.e. democratic self-governance, the market-place of ideas, and individual autonomy. Therefore, restrictions on such speech in the Wang Fei case are justifiable and desirable.

In sum, the harms from the human flesh search engine targeting private individuals are extremely serious, and preventing these harms and protecting privacy could be a compelling interest. As a result, restrictions on online speech about private individuals and of private concern, if narrowly tailored, can satisfy the compelling interest prong of strict scrutiny, and therefore are constitutional in the U.S. context.[113] When balancing free speech and privacy, speech about private individuals and of private concern deserves relatively less protection, and privacy should be assigned more weight in such cases. The following section discusses how victims of the human flesh search engine can seek remedies for privacy infringement in American law.

IV. REPERCUSSIONS AND REMEDIES IN AMERICAN LAW

A. Various Repercussions Against Victims in the Human Flesh Search Engine

Victims in the human flesh search engine could potentially suffer at least three types of repercussions: reputational damage, economic loss and physical violence.

Firstly, the disclosure of personal information in the human flesh search engine can readily lead to damage of one's reputation. The gravity of social stigma depends upon the strength and pervasiveness of the mobilized hostility,[114] which is rooted in the

---

[113] Many states either have enacted laws against offensive online speech or established task forces to create such laws. *See* Harry A. Valetk, *Cyberstalking: Navigating a Maze of Laws*, N.Y. L.J., July 23, 2002, at 5. Admittedly, the "narrowly tailored" prong does raise concerns about restrictions of online speech. For instance, Utah's recent proposed anti-doxing bill was considered to be too over-board to pass the First Amendment scrutiny. *See* Eugene Volokh, *Utah 'Anti-Doxxing' Bill Would Outlaw Mentioning a Person's Name Online 'With Intent to Offend'*, WA. POST (Feb. 8, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/08/utah-anti-doxxing-bill-would-outlaw-mentioning-a-persons-name-online-with-intent-to-offend/ [https://perma.cc/P5RL-GWEQ] (stating the opinion that being unable to call someone "foolish" would be too restricting on the First Amendment). If the proposed law is too broad, it could hardly pass the First Amendment; if too narrow, it would not provide sufficient relief for a victim of online offensive speech.

[114] Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 51–52, (discussing the social

social and moral tolerance of a given time and context. Moreover, the disclosure of personal information in the human flesh search engine almost certainly leads to cyber harassment. In addition to endless disruptive telephone calls, the Internet makes it easier for people to engage in malicious accusations, defamation, slander, and libel. All these kinds of reputational harms can be found in the Wang Fei case.[115]

Second, the human flesh search engine can also inflict serious damage on the target's ability to gain or maintain employment, thereby causing economic harm to them. In the Wang Fei case, the human flesh search engine resulted in Wang Fei losing his job, and foreclosed future employment for an extended period of time.

Last but not least, disclosure of personal information about targets with socially and morally unacceptable behaviors leads to physical violence. The personal information disclosed in the human flesh search engine about targets serves as a tacit invitation of hostility to those Internet users, who, being already engaged in the human flesh search engine, have the potential to 'go extreme.' This is what happened in the Wang Fei case.[116]

B. Torts Remedies in American Law

Victims of the human flesh search engine can seek torts remedies for the repercussions, which involve three distinct privacy torts under American law: public disclosure of private facts,[117]

---

sanctions against communists in the McCarthy era, which was triggered by public disclosure of private facts).

[115] *See supra* Part II (describing the Wang Fei case in detail).

[116] *See supra* Part II (describing the Wang Fei case in detail). Similarly, the exposure to parents and husbands of the identity of women seeking abortion can result in unwanted and unwarranted action of violence, threats, and harassment. *See* Planned Parenthood v. American Coalition of Life Activists, 290 F.3d 1058, 1063–66 (9th Cir. 2002).

[117] Past cases in American law have established that "lack of newsworthiness is an element of the 'private facts' tort, making newsworthiness a complete bar to common law liability" for the tort of public disclosure of private facts. Shulman v. Group W Productions, *Inc.*, 955 P.2d 469, 478 (1998). In the Wang Fei case, although the incident of suicide itself is clearly newsworthy, Wang Fei's personal information, such as his cellphone number, home address and national identity number, is not. The primary reason for this is that the connection between the activities that brought Wang Fei into the public eye and the particular personal information that was disclosed is too weak. Thus, the publication of such personal information may well constitute the common law tort of public disclosure of private facts.

intrusion upon seclusion,[118] and false light.[119, 120] The more challenging questions is: who should be liable for privacy torts?

If the common law tort liability were established, Wang Fei is entitled to seek judicial remedies against three defendants, each of whom represents a distinct type of stakeholder of the human flesh search engine. The first defendant, Zhang Leyi, is merely a private blog owner on the Internet. But unlike conventional media channels, through reposting and hyperlinking, the size of the audience of his publication is significantly increased by the Internet.[121] Zhang Leyi is the owner of his personal blog website (orionchris.cn), on which he posted stories about Jiang Yan and Wang Fei. These blogs also included personal information about Wang Fei and defamatory statements against him and his mistress. His personal website can be regarded as an Internet content provider and he is one of the most notable participant of the human flesh search engine against Wang Fei. Such direct infringement could hardly escape liability.

The second defendant, Tianya, was the most popular Chinese BBS, almost all content of which is generated by the website's millions of registered users. Internet users are allowed to communicate publicly by posting messages on Tianya's BBS, where

---

[118] Under the tort of intrusion upon seclusion, liability may be imposed for an intrusion into a "private place, conversation, or matter . . . in a manner highly offensive to a reasonable person." *Id.* at 230. In the Wang Fei case, some Internet users had intruded into private matters by obtaining private information from non-public sources (e.g. Wang Fei's private photos). Furthermore, telephone harassment and physical intrusion into Wang Fei's home might well constitute the common law tort of intrusion upon seclusion.

[119] In common law torts, one who publicizes a matter concerning another that places that person before the public in a false light is subject to liability to that person for invasion of his privacy. Lovgren v. Citizens First National Bank, 534 N.E.2d 987, 991–92 (Ill. 1989). As previously discussed, through social cascades and group polarization, online speech in the human flesh search engine can be very polarizing and highly offensive to the target. In the present case, building on the fact that Wang Fei committed adultery, some Internet users, as well as Daqi, portrayed Wang Fei in a false light in order to depict him as a guilty, indecent, and disgraceful man in every aspect of his life. Thus, the common law tort of false light might well sustain in cases involving the human flesh search engine.

[120] William Prosser identified four distinct privacy torts that had developed through the 300 cases based on the Warren and Brandeis article. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 388–89 (1960). The privacy torts are (1) public disclosure of private facts, (2) intrusion upon seclusion, (3) false light, and (4) appropriation. For recent discussion and cases about privacy torts, see generally ANITA ALLEN, PRIVACY AND SOCIETY ch. 1 (2d ed. 2011) (describing current privacy tort cases).

[121] For more discussion about information distribution of individual Internet users, see LAWRENCE LESSIG, REMIX: MAKING ART AND COMMERCE THRIVE IN THE HYBRID ECONOMY 46–50 (2008); YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 1-7 (2006).

content can be read by any Internet users. Internet users conducted the human flesh search engine and posted commentaries on Tianya. Should Tianya be liable for the illegality of the human flesh search engine in American jurisprudence?

To answer this question, we must first examine liability of Internet intermediaries under the U.S. law. In order to promote competition in the telecommunication industry and to prevent indecent material from transmitting via computers and phone lines, the U.S. Congress passed the Telecommunication Act of 1996.[122] Title V of the Telecommunication Act was codified as the Communication Decency Act. Section 230(c)(1) of the Communications Decency Act provides, "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[123] Section 230 immunity is the most important safe harbor for intermediary liability of interactive computer service providers.[124]

Since the promulgation of Section 230, litigation has promptly followed this liability vacuum for offensive online speech. Although the U.S. Supreme Court has not yet directly addressed the liability of Internet service providers, lower courts have, in a number of cases, upheld this provision and given relatively broad interpretation of this immunity.[125]

The seminal decision in the United States is Zeran v. America Online, Inc. ("AOL").[126] There, an unidentified third party posted messages on AOL, advertising t-shirts with tasteless slogans related to the bombing of the Oklahoma City federal building, as well as Zeran's phone number. This resulted in Zeran being inundated with

---

[122] Telecommunications Act of 1996, Pub. L. No 104-104, 110 Stat. 56 (1996).

[123] 47 U.S.C. § 230(c) (1998).

[124] Jack Balkin argues that section 230

> [H]as had enormous consequences for securing the vibrant culture of freedom of expression we have on the Internet today . . . .Section 230 is by no means a perfect piece of legislation; it may be overprotective in some respects and underprotective in others. But it has been valuable nevertheless.

Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 434 (2009).

[125] *See, e.g.*, Zeran v. America Online, Inc., 129 F.3d 327, 330–35 (4th Cir. 1997); Barrett v. Rosenthal, 40 Cal. 4th 33, 42–58 (2006); Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413, 419–22 (1st Cir. 2007); Directory Assistants, Inc. v. SuperMedia, LLC et. al., 884 F. Supp. 2d 446 (2012).

[126] Zeran v. America Online, Inc., 129 F.3d 327, 330–35 (4th Cir. 1997).

death threats and other violent calls and text messages. Zeran brought an action against AOL, arguing that AOL unreasonably delayed in removing defamatory messages. Zeran contended that "once he notified AOL of the unidentified third party's hoax, AOL had a duty to remove the defamatory posting promptly, to notify its subscribers of the message's false nature, and to effectively screen future defamatory material."[127] The Zeran Court held that Section 230 immunized interactive computer service providers from claims based on information posted by a third party.[128]

The Zeran Court provided two main reasons. First, the Zeran Court recognized that interactive computer services have millions of users and that the amount of information communicated via interactive computer services is "staggering."[129] It would be impossible for service providers to screen millions of postings for potential tort liability.[130] The Zeran Court refused to apply notice-based liability for the concern that Internet service providers would face potential liability each time they receive notice of a potentially defamatory statement—from any party, concerning any message.[131] Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information.[132] In light of the vast amount of speech communicated through interactive computer services, these notices could produce an impossible burden for service providers, who would be faced with ceaseless choices of suppressing controversial speech or sustaining prohibitive liability.[133]

---

[127] *Id.* at 330.

[128] *Id.* Zeran made another, though ultimately unsuccessful, attempt to seek remedy from a classic-rock radio broadcaster, which redistributed the defamatory content. *See* Zeran v. Diamond Broad, Inc., 203 F.3d 714, 718–22 (10th Cir. 2000) (describing the appeal).

[129] Zeran v. America Online, Inc., 129 F.3d 327, 331 (citing Reno v. ACLU, 521 U.S. 850).

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.* at 333. Notably, subsequent cases viewed Zeran as the foundation of a principle establishing absolute immunity for Internet service providers under section 230 and refused to apply notice-based liability by repeatedly emphasizing the undue burden that would be created by the application of notice-based liability. *See, e.g.*, Doe v. America Online, Inc. 783 So.2d 1010, 1013–1017 (Fla. 2001); *Schneider v. Amazon.com, Inc.* 108 Wash.App. 454, 31 P.3d 37 (2001); PatentWizard, Inc. v. Kinko's Inc. 163 F.Supp.2d 1069, 1071–1072 (D.S.D.2001); Blumenthal v. Drudge 992 F.Supp. 44, 49–52 (D.D.C.1998).

Moreover, potential liability for each message republished by their services might create chilling effects, that is: Internet service providers "might choose to severely restrict the number and type of messages posted".[134]

According to Zeran, interactive computer service providers can enjoy Section 230 immunity under the U.S. law. Could Tianya and Daqi be categorized as interactive computer service providers? Section 230 defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."[135] In analyzing the availability of the immunity offered by Section 230, U.S. courts generally apply a three-prong test: (1) the defendant must be a provider or user of an "interactive computer service," (2) the asserted claims must treat the defendant as a publisher or speaker of the harmful information at issue, and (3) the information must be provided by other "information content provider."[136]

In this case, Tianya is the provider of BBS service (interactive computer service), on which some Internet users (publishers or speakers) spread harmful information about Wang Fei. Tianya, therefore, satisfied all three prongs of the test, thus can be regarded as an interactive computer service provider under Section 230. Consequently, Section 230 would immunize Tianya from liability for information that originates with other users of the human flesh search engine.

The last defendant, Daqi, is a commercial online news agency that functions as a traditional printing press. Daqi published a news column about the incident, in which it not only compiled and reposted other news sources, but also generated its own content, such as an interview with Jiang Hong (Jiang Yan's sister) and Zhang Leyi, a summary of online criticism, an interview with a psychologist, etc. Therefore, Daqi is not only an Internet service provider but also an information content provider, which directly posted content that infringes Wang Fei's privacy.

---

[134] Zeran v. America Online, Inc., 129 F.3d 327, 331 (4th Cir. 1997).
[135] 47 U.S.C. § 230(f)(2) (1998).
[136] Schneider v. Amazon.com, Inc., 31 P.3d 37, 39 (Wash. Ct. App. 2001).

According to Section 230, an information content provider is: "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[137] Section 230 immunity extends only when the content is not provided by the service entity, and Internet content providers do not enjoy Section 230 immunity.[138] In the Wang Fei case, Daqi exercised its editorial discretion and made substantial contribution to the content at issue, making it an Internet content provider. Therefore, Daqi cannot claim immunity for content it created and distributed under Section 230. In short, under American jurisprudence, Daqi would also be held liable for infringing on Wang Fei's right to privacy.[139]

V. POLICY IMPLICATIONS FOR REGULATING THE HUMAN FLESH SEARCH ENGINE

The goal of this Note is not only to argue that the value of privacy trumps the value of free speech when online speech in the human flesh search engine is about private individuals and of private concerns, but also to examine possible remedies for the victims of the human flesh search engine. Based on previous analysis in American jurisprudence, this section examines policy implications for Chinese policymakers.

The first question is who should be liable for the human flesh search engine? A victim of the human flesh search engine generally has two options.[140] The first option is to pursue legal remedy against those Internet users who, as a matter of positive law, are directly

---

[137] 47 U.S.C. § 230(f)(3) (1998).

[138] An information content provider has no immunity under Section 230. *See, e.g.*, Fair Hous. Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921, 926 (9th Cir. 2007) (holding that by creating and developing a discriminatory questionnaire, Roommates.com made itself an information content provider with no immunity under section 230).

[139] As Justice Harlan rightly pointed out in *Time v. Hill*, "[o]ther professional activity of great social value is carried on under a duty of reasonable care, and there is no reason to suspect the press would be less hardy than medical practitioners or attorneys, for example." Time v. Hill, 385 U.S. 374, 410 (1967). Because of the wide coverage and the interactivity, a higher standard of professional responsibility should be applied to online news agencies than traditional press outlets in order to properly prevent potential harm to private individuals.

[140] Some victims of the human flesh search engine chose to remain silent because seeking remedies publicly might bring more public attention, thus risking further exposure and harassment.

responsible for online tortious infringement. But this lacks any meaningful chance of success for two reasons. First, when engineers designed what became the Internet, they chose not to incorporate an identification layer into the entire network architecture.[141] Such technological design makes most online speech anonymous.[142] Because of the anonymous nature of the Internet, it is very difficult to locate the speakers in the human flesh search engine, let alone to punish them.[143] Furthermore, the Internet allows oversea Internet users to participate in the human flesh search engine, and seeking remedies against them is particularly difficult, if not impossible. This, of course, does not mean that those offending Internet users should escape accountability.[144] Still, most participants of the human flesh search engine are effectively liability-proof.

A more effective, practical option is to hold the Internet intermediaries liable.[145] That is to sue the Internet intermediaries who directly participate in the human flesh search engine or indirectly provide the platforms for users to conduct the human flesh search engine. From the perspective of the victims, Internet intermediaries are not only easier to find, but also have deeper pockets and are thus

---

[141] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 31–33 (2008); David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J. L. & TECH. 9, 82 (2004).

[142] Although some countries (such as South Korea and China) have attempted to implement real-name systems in the Internet, there are always technological solutions that can be used to circumvent such systems and to maintain anonymity.

[143] Lyrissa Barnett Lidsky, *Silencing John Doe: Defamation & Discourse in Cyberspace*, 49 DUKE L.J. 855, 859 (2000) ("[T]he typical John Doe [defendant] has neither deep pockets nor libel insurance from which to satisfy a defamation judgment.").

[144] In the United States, prosecutors have attempted to employ the Computer Fraud and Abuse Act, which was originally designed to punish and deter hackers from breaking into computer systems to obtain private information, to prosecute cyberharassers. *See, e.g.*, Linda Deutsch, *Teen's Neighbor Charged in Death*, WASH. POST, C3 (May 16, 2008).

[145] Many commentators suggest holding Internet service providers liable for online infringement. *See, e.g.*, SOLOVE, *supra* note 81, at 149–59; Nancy S. Kim, *Web Site Proprietorship and Online Harassment*, 2009 UTAH L. REV. 993, 1026-33 (2009); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1010-15 (2008); Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 108–10, 112–13 (2007); Daryl J. Levinson, *Aimster and Optimal Targeting*, 120 HARV. L. REV. 1148, 1154 (2007); Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 233–40 (2006); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1095–1101 (2001); Brian McManus, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647, 661–68 (2001).

more financially attractive targets for litigation.[146] More importantly, as some commentators note, Internet intermediaries are in a better position to monitor and deter online infringement at lower costs.[147]

The more challenging question is which liability regime shall be adopted for Internet intermediaries? In the United States, although Internet content providers are likely to be held liable for online infringement, Section 230 provides almost absolute immunity to Internet service providers, and only a number of legal claims (such as copyright infringement) [148] can pierce such immunity. [149] As demonstrated below, if China were to take this approach, victims of the human flesh search engine would lack meaningful redress. Modestly reforming the absolute immunity shield could give them effective options. The author argues that the notice-based liability against Internet service providers, which is being used in the online copyright regulation in the United States, is more effective than absolute immunity in regulating the human flesh search engine.

First, when Section 230 was passed twenty years ago, the oft-cited argument for Section 230 immunity was that the Internet was a young industry and Section 230 was established to "maintain the robust nature of Internet communication" and to "preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services." [150] But today, the Internet industryhas become mature, robust and much more financed.[151] They are now capable, and socially responsible, to spend money and

---

[146] *See* Scot Wilson, *Corporate Criticism on the Internet: The Fine Line Between Anonymous Speech and Cybersmear*, 29 PEPP. L. REV. 533, 555 (2002) (stating most plaintiffs in "cybersmear" campaigns would rather sue those who can pay more, i.e. the Internet service providers).

[147] Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 237 (2006).

[148] In the United States, the copyright industry (especially the Recording Industry Association of America and its analogue in the movie industry, the Motion Picture Association of America) has spent great effort in limiting section 230 immunity since its promulgation. This is not a novel phenomenon in the history of intellectual property law. As William Landes and Richard Posner demonstrate, the political forces that favor intellectual property right owners contributes to the increase of intellectual property protection since 1976. WILLIAM M. LANDES & RICHARD A. POSNER, THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY LAW 25 (2004).

[149] 47 U.S.C. § 230(f) (1998).

[150] 47 U.S.C. § 230 (1998); *see generally* 141 Cong. Rec. H8470 (August 4, 1995) (explaining legislative purposes).

[151] YOO, *supra* note 6, at 128–34.

manpower on screening and filtering illegal content—they have already done this for online copyright infringement.

Second, absolute immunity might well create disincentives to Internet intermediaries in developing new kind of self-regulating technologies or services that might threaten their existing way of doing business. For example, in the United States, AT&T was uninterested in developing Internet technologies decades ago because doing so would threaten its control of the phone system.[152] Indeed, under an absolute liability regime, Internet intermediaries' best strategy is to remain passive and abstain from incurring any cost of deploying affirmative technologies or services. However, notice-based liability might well give incentives for Internet intermediaries, especially those wealthy ones, to develop detecting, filtering, and abuse-reporting mechanisms to weed out potential offensive online speech in the human flesh search engine.

This has been proved in the area of online copyright protection. The U.S. Congress provided strong incentives under Section 512 of Digital Millennium Copyright Act for Internet service providers to take down access to websites that were allegedly violating copyright.[153] With the notice-based liability imposed by Section 512, Internet intermediaries were impelled to develop various kinds of viable copyright protection technologies, such as digital watermarking, digital fingerprinting, and digital rights management systems, which have made a substantial progress in detecting and preventing plagiarism and copyright violations. Similarly, imposing a notice-based liability in the area of online privacy protection can incentivize the Internet industry to develop technological solutions to monitor and filter privacy infringement content, thereby alleviating the problem of the human flesh search engine.

Exercising editorial control and judgement over its services is not uncommon for Internet service providers, and it can be beneficial to them. Of course, the Internet has lowered the costs of content transmission and distribution, thereby increasing the participation by a large number of Internet users. However, the proliferation of offensive speech about private individuals and of private concerns is of little value to societal wellbeing. When this offensive speech

---

[152] LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD 31–33 (2002).

[153] LAWRENCE LESSIG, FREE CULTURE: THE NATURE AND FUTURE OF CREATIVITY, 190–91 (2004).

occupied the front pages, it would likely decrease the visibility of valuable discussion and make the entire online community less trustworthy and accountable. Thus, the online world would become less attractive to Internet users. This is why most BBS administrators monitor the online community and delete useless postings such as unwanted solicitation and personal insults.

Tianya itself is an example. According to Tianya's "User Agreement," users of Tianya are required to refrain from posting certain content including solicitation, obscenity, hate speech, libel, rumors, etc. Tianya is allowed to remove these online postings without informing their users.[154] Moreover, Tianya, like other major BBS in China, utilizes both human monitors and screening technologies, which prescreens BBS postings for illegal and offensive language.[155] In other words, unlike traditional news vendors and bookstores, Tianya has the ability to continually monitor online postings and in fact does spend time and effort for censoring online postings. This ability is amplified by the growth of its monitoring team and the development of the data analytical technologies. Tianya's decision to regulate the content of its BBS was partially influenced by the existing political speech control in China, and partially incentivized by its own desire to attract a market consisting of users seeking a user-friendly BBS environment.

Indeed, some of these monitoring and filtering strategies would actually benefit the Internet service providers themselves. Internet users are more likely to choose Internet services that are more credible (such as editing entries in Wikipedia) or more user-friendly (such as filtering spams in email service). Because of this, regulating content in the human flesh search engine could make the online service less offensive and more trustworthy to Internet users. In the long run, it would help to build a better online environment that would benefit Internet service providers.

Third, Section 230 removes liability from Internet service providers, which would in turn encourages Internet service providers to take reckless actions and allows Internet service providers to turn

---

[154] Tianya Yonghu Xieyi (天涯用户协议) [Tianya's User Agreement], http://service.tianya.cn/guize/regist.do [https://perma.cc/7P6R-CH4Y] (last visited Nov. 22, 2016).

[155] CONG.-EXECUTIVE COMM'N ON CHINA, BLOCKING, FILTERING, AND MONITORING, http://www.cecc.gov/blocking-filtering-and-monitoring [https://perma.cc/68UE-WJ9P] (last visited Nov. 22, 2016).

a blind eye to problems.[156] The Ninth Circuit noted in Batzel v. Smith that "the broad immunity created by Section 230 can sometimes lead to troubling results," such as providing no incentive for a website owner to take down a post after being informed it is defamatory nature.[157]

This leads to the final point: absolute immunity to Internet service providers would leave victims of the human flesh search engine vulnerable and helpless. One might argue that victims, in one way or another, can seek judicial remedies by filing a civil action. Such remedies, however, suffer from both legal and practical defects. As a legal matter, the damage is difficult to be evaluated during the course of the human flesh search engine. This is especially so considering that data on the Internet is almost impossible to be completely deleted. The scope of legal relief available is thus greatly constrained. As a practical matter, the remedies become even more difficult to achieve. As discussed above, the anonymous nature of the Internet make it almost impossible to track down all the violators. Even if the violators were eventually identified, legal action against them requires the expenditure of time and effort, while ultimate vindication may be long delayed and bring little relief to victims of the human flesh search engine under the Chinese legal system.

One of the most powerful criticism against notice-based liability for Internet service providers is that they would have incentives to simply remove all messages for which they receive notice of defamatory content because they face liability for maintaining the message but not for removing it. This so-called "Proxy Censorship" or "Collateral Censorship" would raise a First Amendment concern in the U.S. context.[158] Nonetheless, opponents underestimate a factor that the business model of most Internet service providers is predicated on large volumes of traffic and data

---

[156] Ann Bartow, *Internet Defamation as Profit Center: The Monetization of Online Harassment*, 32 HARV. J.L. & GENDER 383, 418 (2009); *see also* SOLOVE, *supra* note 81, at 159.

[157] Batzel v. Smith, 333 F.3d 1018, 1031 (9th Cir. 2003).

[158] *See* Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 27–9 (2006); Jack M. Balkin, *Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds*, 90 VA. L. REV. 2043, 2095–98 (2004); Jack Balkin, *Free Speech and Hostile Environments*, 99 COLUM. L. REV. 2295, 2296–2305 (1999); Michael I. Meyerson, *Authors, Editors, and Uncommon Carriers: Identifying the "Speaker" Within the New Media*, 71 NOTRE DAME L. REV. 79, 116, 118 (1995).

flowing through their services, which incentivizes these Internet service providers to generate as much traffic and data as possible.[159] As a result, the profit-maximizing Internet service providers are more likely to allow the dissemination of gossip, rumor, and personal information, even if they are vicious, aggressive and harmful, rather than removing all suspicious content. This is especially seen in the human flesh search engine, where infringing content is typically not marginal, and usually serves as a draw that attracts large Internet audiences and traffic. In other words, the business model incentivizes Internet service providers to try their best to utilize the content of the human flesh search engine in order to promote Internet traffic through their servers. Furthermore, market forces will discipline massive removal of online content.[160] The human flesh search engine always involves multiple online communities at the same time. Since there are alternative online communities, Internet users can simply change Internet service providers if their posts were repeatedly removed at a particular online community. Last but not least, as discussed above, the speech in the human flesh search engine deserves less First Amendment protection.[161]

Indeed, compared to absolute immunity, notice-based liability provides some disincentives for Internet service providers to conduct massive removal of online content; compared to strict liability,[162] notice-based liability provides a warrant of proportionality in regulating online speech.[163] Having said that, we need to caution against imposing too high of a burden to Internet service providers, which will be reflected in the below policy recommendations.

---

[159] As Paul Ohm notes, Internet service providers attempts to replicate Google's successful utilization of behavioral data, which are being turned into advertising revenue. *See* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1426 (2009) (explaining Google's success and the response to Google's success).

[160] Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 252 (2006).

[161] *See supra* Part III, Sections B and C (explaining that some speech receives less protection than others and why).

[162] *See* Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901, 916 (2002) (elaborating that strict liability for Internet service providers can cause over-deterrence and over-censorship).

[163] An accompanying policy is the counter-notice and put-back procedures. Both China and the U.S. has the same kind of policy in online copyright regulation. *See* 17 U.S.C. §512(g) (2010); Xinxi Wangluo Chuanboquan Baohu Tiaoli (信息网络传播权保护条例) [Regulation on the Protection of the Right to Communicate Works to the Public Over Information Networks] (promulgated by the St. Council, May 18, 2006, amended on Jan. 30, 2013), art. 16, 17.

In the Wang Fei case, the Beijing Chaoyang District Court actually applied the notice-based liability and held one of the Internet service providers liable.[164] The Beijing Chaoyang District Court maintained that, as a condition for limited liability, Internet service providers must expeditiously take down the content they host when they are notified of the alleged illegality.[165] The Beijing Chaoyang District Court followed the analogy of the notice-based liability, and held that Daqi failed to fulfill the take-down obligation and thus were liable.[166] Following the same rationale, since Tianya took down the disputed threads and posts in a "timely" manner upon receiving the removal request from Wang Fei, it would not be liable for the privacy infringement in this case.[167]

Later in the year, this notice-based liability regime was established in the newly promulgated Tort Law of the PRC, under which Internet intermediaries would be held liable if they failed to take necessary action upon receiving notice from the victim or it has the knowledge of the online infringement.[168] This notice-based

---

[164] The Wang Fei case is the first case where Chinese Courts held Internet service providers liable in the human flesh search engine. However, Chinese Courts have previously held Internet service providers liable in online copyright infringement cases. *See, e.g.*, Beijing Ciwen Yingshi Zhizuo Youxian Gongsi Su Guangzhou Shulian Ruanjian Jishu Youxian Gongsi (北京慈文影视制作有限公司诉广州数联软件技术有限公司) [Beijing Ciwen Studio Inc. v. Guangzhou Shulian Software Technology Co. Ltd.], (Guangzhou Higher People's Ct. 2006); Zhejiang Fanya Dianzi Shangwu Youxian Gongsi Su Beijing Yahuwang Zixun Fuwu Youxian Gongsi, Beijing Alibaba Xinxi Jishu Youxian Gongsi (浙江泛亚电子商务有限公司北京雅虎网咨询服务有限公司，北京阿里巴巴信息技术有限公司) [Zhejiang Flyasia E-business Co., Ltd v. Beijing Yahoo! Consulting and Service Co., Ltd. & Beijing Alibaba Information Technology Co. Ltd.], (Beijing No. 2 Interm. Ct. Dec. 15, 2006); Shanghai Busheng Yinyue Wenhua Chunabo Youxian Gongsi Su Beijing [FashioNow] Gongsi (上海步升音乐文化传播有限公司诉北京公司) [Shanghai Push Sound Music & Entm't. Co., Ltd. v. Beijing FashioNow Co.], (Beijing No. 2 Interm. Ct. Dec. 19, 2006); Guangzhou Shulian Ruanjian Jishu Youxian Gongsi Su Guangdong Zhongkai Wenhua Fazhan Youxian Gongsi (广州数联软件技术有限公司诉广东中凯文化发展有限公司) [Guangzhou Shulian Software Technology Co., Ltd. v. Guangdong Zoke Culture Development Co., Ltd.], (Shanghai Higher People's Court Feb. 21, 2008). For more discussion about intermediary liability of online copyright infringement in China, see Ke Steven Wan, *Internet Service Providers' Vicarious Liability Versus Regulation of Copyright Infringement in China*, U. ILL. J.L. TECH. & POL'Y 375, 389–99 (2011).

[165] Wang Fei Su Daqi Wang, *supra* note 37.

[166] *Id*.

[167] Wang Fei Su Tianya, *supra* note 47.

[168] Article 36 of Tort Law provides that:

> Internet users and internet service providers shall bear tortious liability in the event they infringe other people's civil rights and interests through the internet. Where an internet user engages in

liability regime was further established in the Decision Concerning Strengthening Network Information Protection of 2012.[169]

However, the court's decisions are not without criticism. The most crucial one is that the Beijing Chaoyang District Court did not specify the reasonable time-frame for the take-down action. In the Wang Fei case, it took Tianya more than three months to take down the relevant postings. Considering the speedy dissemination of information on the Internet, Wang Fei can still argue that Tianya's take-down action is not "timely" at all.

Therefore, in order to better regulate the human flesh search engine, the first policy recommendation to Chinese policymakers is to specify the time-frame for notice-based liability. The law could provide a more concrete standard to determine whether Internet

---

> tortious conduct through internet services, the injured party shall have the right to inform the internet service provider that it should take necessary action such as by deleting content, screening, breaking links, etc. Where an internet service provider fails to take necessary action after being informed, it shall be jointly and severally liable with the internet user with regard to the additional injury or damage suffered. Where an internet service provider knows an internet user is infringing other people's civil rights and interests through its internet service but fails to take necessary action, it shall be jointly and severally liable with the internet user.

Qinquan Zeren Fa (侵权责任法) [Tort Law] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010), official full text, in Chinese, available at: http://www.gov.cn/flfg/2009-12/26/content_1497435.htm [https://perma.cc/38EY-RJL2].

[169] Article 8 of the decision provides that

> Where citizens discover that their individual identity has been divulged, individual privacy has been disseminated or other network information infringes their lawful rights and interests, or are harassed by commercial electronic information, they have the power to require the network service provider to delete the relevant information or adopt other necessary measures to cease this.

Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Guanyu Jiaqiang Wangluo Xinxi Baohu de Jueding (全国人民代表大会常务委员会关于加强网络信息保护的决定) [National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 28, 2012, effective Dec. 28, 2012), http://www.gov.cn/jrzg/2012-12/28/content_2301231.htm [https://perma.cc/8QCJ-PRHW. To date, this decision is the highest level law in China to regulate online privacy infringement. Violation of the notice-based liability standard may lead to warnings, fines, confiscation of illegal income, cancellation of operation permits, shut-down of websites, or the prohibition of involved entities from engaging in other network services business.

service providers take down infringing content in a timely manner. Infringing content in a human flesh search engine is usually time-sensitive. As a general rule, such content is most devastating immediately after the incident. With the passage of time, the value of content diminishes. As a result, if the infringing content were available for a relatively long time, by the time such content is finally taken down, the take-down action may well be less meaningful. Such time-frame shall be subject to the best available technologies (particularly, the ex-ante detecting, filtering and ex-post reporting, deleting technologies) in a given time.

Second, since undue burden is a concern, when applying notice-based liability against Internet service providers, policymakers need to limit unnecessary take-down requests.[170] Naturally, the victims are better positioned to determine whether information about him or her is infringing or defamatory. The law could place some burden of the exercise of notice against the victims. For example, the law could require victims to provide the real identity of themselves, to bear the burden of demonstrating that the online speech at issue is illicit, to provide accurate information about the alleged infringement, and to file the complaints through an authorized, designated system or a licensed lawyer.[171] In practice, this might well increase the

---

[170] Perhaps the best recent illustration of this concern in the United States can be found in the Zeran case. *See Zeran*, 129 F.3d 327, 333 (discussing the risk of strategic "notice" to ISPs to suppress content). For information on cases regarding the potential abuses of notice and take down system in China, see Si Xiao & Fan Luqiong (司晓 & 范露琼), Tengxun Yanjiuyuan (腾讯研究院) [Tencent Research Institute], Zhishi Chanquan Lingyu "Tongzhi – Shanchu" Guizi Lanyong de Falv Guizhi) (知识产权领域"通知—删除"规则滥用的法律规制) [Legal Regulation Against Abuse of "Notice and Take-Down" Rules in Intellectual Property Area] (2015), http://www.tencentresearch.com/4014 [https://perma.cc/A9PY-QESD].

[171] Similar legislative efforts have been made in online copyright regulation. *See* Zuigao Renmin Fayuan "Guanyu Shenli Sheji Jisuanji Wangluo Zhuzuoquan Qinquan Jiufen Anjian Shiyong Falv Ruogan Wenti de Jieshi" (最高人民法院《关于审理涉及计算机网络著作权侵权纠纷案件适用法律若干问题的解释》) [Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Laws in Hearing Cases Involving Computer Networks Copyright Dispute] (promulgated by the Sup. People's Ct., Nov. 22, 2000, first amendment made on Dec. 22, 2003, second amendment made on Dec. 8, 2006) (When filing a complaint or a notice to Internet service provider, article 7 of the Interpretation requires copyright owners to provide identity certification, proof of copyright ownership, and proof of copyright infringement.). *See also* Xinxi Wangluo Chuanbo Quan Baohu Tiaoli (信息网络传播权保护条例) [Regulation on the Protection of the Right to Communicate Works to the Public over Information Networks] (promulgated by the St. Council, May 18, 2006, amended on Jan. 30, 2013) (providing in article 14 that copyright owners are entitled to submit written notification to the Internet service providers about alleged infringement, and that the notification shall include (1) the name, contact information

accuracy of the complaints, the efficiency of the review process, and prevent the abuse of such notice-based liability. In the meantime, doing so would also help alleviate the risk-averse disposition by Internet intermediaries such as deleting too much lawful content upon receiving notices.[172]

Third, Internet intermediaries shall be incentivized to cooperate with victims and law enforcement agencies—a cooperation towards an optimal mechanism to address the problems of the human flesh search engine. Internet intermediaries usually have access to some sorts of information about their subscribers such as registration information and IP addresses. As a result, Internet intermediaries are often in a better position to help locate and investigate the offensive Internet users who are allegedly engaging in the human flesh search engine.[173] This may greatly reduce the cost for detecting and deterring the human flesh search engine.

Most victims of the human flesh search engine lack financial wherewithal to engage in lengthy and expensive public reputation management or legal battles. They have a greater need of assistance from Internet intermediaries in order to timely cease infringement or seek remedies. Wealthy victims of the human flesh search engine may hire a public reputation management company that specializes in removing damaging online content or launching legal battles. However, the chances of success of such action also highly depend on cooperation with relevant Internet intermediaries.

Admittedly, such cooperation is a burden for Internet intermediaries; but in a long run, Internet intermediaries would benefit from having a healthier and cleaner online community. The law could encourage closer cooperation between the Internet intermediaries, victims and law enforcement, which would better

---

and address of copyright owners; (2) the name and web link of the infringing content; and (3) proof of copyright infringement).

[172] As some commentators noted, liabilities will tend to increase incentives of risk-adverse entities to over-comply. *See* John E. Calfee & Richard Craswell, *Some Effects of Uncertainty on Compliance with Legal Standards*, 70 VA. L. REV. 965, 986 (1984) (explaining biased damage awards).

[173] *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 236–38 (2006) (arguing that Internet service providers are usually capable to detect, deter, or otherwise influence the illicit acts in question at low costs); Daryl J. Levinson, *Aimster and Optimal Targeting*, 120 HARV. L. REV. 1148, 1154 (2007) (explaining that when a third party is better positioned to monitor and control of the primary wrongdoer, imposing indirect liability against the third party will be more efficient).

help victims in the human flesh search engine and punish the offensive Internet users.

Finally, let us not forget the analysis of the tension between privacy and free speech as discussed above. The law should consider the distinction between private individuals and notable public figures. Speech of public concerns and of private concern shall also be taken into account. An incident of the human flesh search engine might well involve multiple parties and multiple affairs, and these nuanced distinction could help better evaluate the situation. Policy makers shall also focus on restrictions on online speech about private individuals and of private concern in the human flesh search engine.[174]

VI. CONCLUSION

In this essay, the author has endeavored to examine the problems of the human flesh search engine by exploring the tension between privacy and free speech in the Internet age. Through legal analysis, we are able to answer the questions set forth in the first Chapter. If online speech is about private individuals (as opposed to public officials and celebrities) and of private concern (as opposed to public concern), the value of privacy should trump the value of free speech. The author does not hold that speech about private individuals and of private concern should not be protected at all. However, when we look closely at the kind of speech in the Wang Fei case and most of the human flesh search engine cases, certain restrictions on such speech are more justifiable. Even in the United States, a jurisdiction where speech is highly protected by the First Amendment, privacy values might well trump speech values in this particular circumstance.

Indeed, Wang Fei suffered a great deal from the human flesh search engine, and he was disproportionally punished in the course of public humiliation and online shaming. In the pre-Internet age, the disclosure of negative personal information among individuals could damage one's reputation but it would fade from memories over time. In ancient China, only those who committed serious crimes might be punished by the practice of the "*Mo*" (punitive face tattooing), one of the Five Punishments for Slaves (*Nu Li Zhi Wu Xing*), in which

[174] *See supra* Part III (discussing the balance of privacy and free speech).

criminals would be tattooed on the face or forehead with indelible ink. Admittedly, even today, criminal cases may involve shaming penalties encouraging social stigmatization of criminal offenders.[175] However, it should be noted that, in a non-criminal case like that of Wang Fei, the brutal practice of face tattooing was brought back in the Internet age, not through the law, but through digital technologies—the 'code.'[176] What otherwise would be a fleeting memory in the minds of a few bystanders are now scrutinized brutally and endlessly on the Internet. And due to the nature of digital technologies, such shaming penalties are inherently difficult to control, which might well constitute a form of mob justice.[177]

When considering liability for Internet intermediaries, policy makers generally have two options: absolute immunity and notice-based liability. Absolute immunity, as illustrated in the United States, would give victims of the human flesh search engine little meaningful likelihood of success in seeking judicial remedies. Instead, notice-based liability to Internet intermediaries, as applied by the Chinese court, can not only offer victims effective options to redress, and but also incentivize Internet intermediaries to self-regulate towards better online communities. In light of these observation and discussion, some recommendations are made to policymakers.

Up to now this essay has provided some basic aspects of the problems of the human flesh search engine and how to address related legal issues. It is impossible to generalize from one case, but the Wang Fei case provides a means to develop an understanding of how networked individuals can be empowered and driven by the human flesh search engine, how to balance the interests of free speech and the interests of privacy, and establishes an expectation for the remedies for the victims of the human flesh search engine. It could become part of a comparative study on regulation of cyberbullying, cyberharassment and cyberstalking. There is a very broad space waiting for further exploration on the tension between privacy and free speech in the Internet age.

---

[175] *See* MARTHA NUSSBAUM: HIDING FROM HUMANITY: DISGUST, SHAME, AND THE LAW 227–50 (2004) (discussing the effects of shaming penalties).

[176] For more discussion about the importance of the 'code,' see LAWRENCE LESSIG, CODE: VERSION 2.0, 1–8 (2d rev. ed. 2006).

[177] James Whitman, *What Is Wrong with Inflicting Shame Sanctions?*. 107 YALE L.J. 1055, 1087–91 (1998).