ABSTRACT: For at least a decade, governments have considered mandating that Web users register their real names and identification numbers with online service providers before posting comments on the providers’ websites. The idea is that real names contribute to responsible speech. Facebook has consistently argued that its real name policy is fundamental to an atmosphere of civility and trust. Citing similar rationales, South Korea and China, have implemented real name registration systems. These three cases allow for insights into the difficulties of implementing a real name system. Given the challenges identified in this paper, real name registration may prove a less potent tool than either its critics or its advocates suggest.

Information spreads farther and faster than ever before due to the global expansion of online social media. Citizens’ ability to access and contribute to real time news cycles has shaken established power structures. An online mirror of social interaction, personal identity, and network building has meant more opportunities for expression. Some forms of expression are dangerous and destructive: Fraudsters, deviants, and terrorists have more effective channels to misrepresent, make others feel insecure, and disrupt social order. Most people agree the world would be improved if malicious speech were prohibited. The practical question is whether it is possible to frame a law preventing such speech without also preventing valuable speech.

States employ a number of methods to exorcise bad speech from the Internet. The tools of the trade are keyword deletion algorithms and human censors that remove online content. For at least a decade, governments have considered mandating systems that require Web users to register their real names and identification numbers with online service providers before posting comments on the providers’ websites. The idea is that real names will contribute to responsible speech.
Facebook, an online platform with more than 1 billion users worldwide, has consistently argued that its real name policy is fundamental to an atmosphere of civility and trust. According to Facebook, “there is no discretion here as the creation of fake accounts threatens the integrity of our whole system.”\(^2\) Citing similar rationales, South Korea and China have implemented systems mandating real name registration in order for netizens to post publicly online.

At some point, liberal political theory holds, enforcement actions outing anonymous Web users reach a certain level of frequency and severity that they have a chilling effect—and not just on bad speech. Critics of the wealthy and powerful, advocates of unpopular views, and whistleblowers often think better of speaking up, knowing that disclosure of their identity may lead to ostracism, imprisonment, or worse. Indeed, real name registration is designed to compliment censorship tools and incentivize citizens to self-censor.

How have real name policies affected online speech? While evidence from South Korea, China, and Facebook is insufficient to draw conclusions about the long-term impacts of real name registration. The cases do allow for insights into the difficulties of implementing a real name system, and these difficulties are formidable. Given the challenges of implementation, real name registration may prove a less potent tool than either its critics or its advocates suggest.

I. **The Cases: South Korea, China and Facebook**

The cases analyze the events leading up to and following the enactment of real name registration laws in South Korea and China, as well as Facebook’s policy. This comparison is not meant to suggest that Facebook has—or should have—duties analogous to a government. The comparison does not equate the distinct political and legal systems of South Korea and China. Each of the three cases discussed, involves
different kinds of social media. For example, the microblogs popular in China are more similar to Twitter than to Facebook. In South Korea, Cyworld, the leading social network, functions as a hybrid of a blog and a personal homepage. The unifying thread is that all cases

A. South Korea: The Future of the Internet?

With its high Internet penetration and state monitoring and surveillance of cyberspace, South Korea may represent the future. South Korea is one of the most wired countries in the world, both in terms of levels of Internet usage and connection speed. Today, 84 percent of the country’s 49 million people use the Internet.³ Online news and networks have permeated everyday social interaction in South Korea, sometimes with devastating effects. Authorities linked at least four celebrity suicides in 2007 and 2008 to online rumors that went viral.⁴

In part due to the country’s legacy of authoritarianism and longstanding national security concerns over North Korean agents and sympathizers, South Korea’s free speech protections are relatively weak compared with many other democracies.⁵ Article 21 of the South Korean constitution guarantees that “all citizens shall enjoy freedom of speech and the press,” but contains the qualification that “neither speech nor the press shall violate the honor or rights of other persons nor undermine morals or social ethics.”⁶ This caveat has empowered the government to impose restrictions on a broad range of expression.

As early as 2003, the Ministry of Information and Communication sought cooperation from South Korea’s four major Web portals (Yahoo Korea, Daum Communications, NHN, and NeoWiz) in developing real name registration systems.⁷ A real name system was first adopted in 2004 as an amendment to the Public Official Election Act.⁸ Incumbent politicians worried about the impact of unregulated online
speech on election outcomes. The law required Web users to verify their identities by submitting their Resident Registration Numbers (a national identification number) before posting to election-related websites.\(^9\)

Over time, the scope of the real name policy widened beyond election related sites. In July 2007, under Article 44-5 of the Act on the Promotion of Information and Communication Network Utilization (the “Network Act”), the South Korean government required all information portals and websites with over 300,000 daily visitors to verify the identity of any Web user posting a comment or uploading video or audio clips on bulletin boards.\(^10\) Korea’s largest Internet portals also independently implemented measures to curb malicious speech. Naver, for example, simplified the process for users to block “groundless rumors or postings.”\(^11\)

The ruling Grand National Party (“GNP”) passed legislation criminalizing “cyber defamation” in July 2008 and initiated a crackdown against bloggers.\(^12\) In one high profile case, Park Dae-sung, using the pseudonym Minerva, posted nearly 300 entries on Daum’s Agora Internet forum between March 2008 and January 2009. He criticized the administration’s economic policy, predicted the demise of Lehman Brothers, and the crash of the won. The South Korean government claimed that his blog posts riled the financial markets, costing the country billions of dollars.\(^13\) Prosecutors filed suit against Park, seeking as many as five years in prison or fines of up to KRW 50 million.\(^14\) Park was arrested and tried but acquitted in April 2009.\(^15\)

In December 2009, the GNP amended Article 44-5 of the Network Act to decrease the threshold for real name registration to all websites with over 100,000 visitors per day.\(^16\) This forced most major South Korean websites to comply.\(^17\) Under the law, online service providers were obligated to disclose personal information of alleged offenders if victims sued for libel or infringement of privacy.\(^18\)
The lowering of the real name registration threshold followed the public relations fiasco faced by President Lee Myung-bak after his decision to resume imports of American beef.\textsuperscript{19} A few months earlier, President Lee had won his election by one of the widest margins in Korean history.\textsuperscript{20} However, by the end of the anti-U.S. beef protests, his popularity stood at a mere 20 percent\textsuperscript{21} and the president’s entire cabinet had offered to resign.\textsuperscript{22} News that U.S. beef would put Koreans at greater risk of bovine spongiform encephalopathy (“BSE” or “mad cow disease”) exploded on the Internet and rippled throughout society before the government could present a counterargument.

The beef issue snowballed into a broader backlash against President Lee’s leadership style and his policies on everything from the economy to North Korea to education reform.\textsuperscript{23} A coalition called the People’s Association for Measures against Mad Cow Disease, including organizations such as the Korean Confederation of Trade Unions and the Korean Teachers’ and Educational Workers’ Union, organized about 100 days of protest—the largest demonstrations seen in Seoul for 20 years.\textsuperscript{24} Over the protest period, Daum’s Agora forum saw page views spike fifty-fold from 40 to 200 million visits per day.\textsuperscript{25} Angry citizens uploaded images and shared information about meeting places, police presence, and arrests via social media, IM, and SMS. A unifying theme among the coalition of protesters was dissatisfaction with the traditional media’s coverage of their grievances. On the Web, a popular refrain summed up this sentiment: “Bring a copy of one of the big dallies with you to the rally. You can sit on it to keep your pants clean.”\textsuperscript{26}

Academic findings analyzing the effects of the real name policy on online speech show mixed results. One study suggested that malicious speech, defined as the number of posts deleted by censors on major portal sites, Daum and Naver,
remained the same (around 5 percent) before and after the real name policy came into force. Other studies observed a decline in online participation and a reduction in the number of violent comments in the immediate days after the 2008 real name policy, but no long-term change.

The real name registration policy did not deter wild and unfounded positions from being promoted online. According to one claim, which appeared to win wide credibility, Koreans were genetically predisposed to mad cow disease. Other online chatter suggested that Korean babies would catch BSE from diapers made with material from U.S. cattle. Students hostile to President Lee’s education reforms warned of a secret deal to use diseased U.S. beef in school lunches.

Uneven application of the law undermined its effectiveness. Google refused to comply with the real name registration system. The U.S. company disabled YouTube video upload and comment functionalities for users accessing the site within South Korea. By changing their country setting users could still upload and comment on the site. This provided a massive loophole and triggered public cynicism about the policy. The Korea Communications Commission decided not to impose penalties on Google and exempted it from the real name law. Other foreign web platforms, such as Twitter, were also exempted. Although Korean online service providers held on to their dominant market position vis-à-vis foreign competitors, they complained that the law caused them to incur additional Web development, monitoring, and security costs that put them at a disadvantage.

Rather than promote Internet security, the real name policy actually introduced new hazards. After recording millions of users’ identification details, websites subject to the real name policy became treasure troves for hackers. According to a report by Korea IT Times, the number of hacking incidents reached “momentous”
proportions in 2011. In one notorious incident, 35 million users of SK Communications’ social network CNS Cyworld had their personal details stolen.

In August 2012, the Korean Supreme Court unanimously struck down the clause of the Network Act that required websites to verify the identifications of users posting comments. The Court reasoned that the real name policy infringed netizens’ rights to freedom of speech, an individual’s right to determine her own personal identity, and online service providers’ rights to freedom of speech. The Court held that public interest must clearly justify restrictions on speech. Evidence did not sufficiently demonstrate a decrease in hateful comments, defamation, and insults on the Internet following the real name policy. Moreover, online service providers could rely upon alternative means to remedy malicious posts, and authorities could track Web users though their IP addresses.

B. China: Witnessing an Unprecedented Platform for Speech

A significant number of the world’s Internet users reside in China, and social media is fast becoming a dominant mode of interaction and information gathering among citizens. There is a digital gap between China’s coastal and interior areas. Internet penetration in Beijing exceeds 70 percent but is less than 25 percent in Yunnan, Jiangxi and other provinces. Overall, China had 513 million Web users, equivalent to roughly 38 percent of the country’s population in 2011, and nearly half of that population used microblogs. The online population is forecasted to grow to 800 million by 2015. Given the Chinese government’s heavy hand in managing the content of established print and broadcast media, microblogs offer a unique space for citizens to obtain and share independent news and gossip.

As early as 2006, the Ministry of Information and Industry had been considering a real name registration system, and the China Internet Trade
Association actively encouraged Internet service providers to require customers to provide identification details in exchange for service. Proponents cited real name registration in South Korea as a positive precedent.

Advocates of the real name policy hoped the law would help prevent online rumors from going viral. Particularly over the two years leading up to the Chinese Communist Party’s (“CCP”) leadership transition at the 18th Party Congress, several incidents highlighted the destabilizing impact of online rumors. In the summer of 2011, for example, when former president and party elder Jiang Zemin failed to show up at celebrations marking 90th anniversary of the founding of the CCP, the online rumor mill predicted Jiang’s death. Online service providers, such as Sina, attempted to rein in the rumors by blocking searches for keywords related to Jiang. Human censors also hand-deleted posts that mentioned the leader. Microbloggers evaded the controls, employing euphemisms and images. Some commentators suggested that the censorship actually encouraged, rather than calmed, the rumors.

Beyond the speculation swirling around the highest-ranking party officials, online discussion became an outlet for pent-up social frustrations. In 2011, the blogosphere fixated on a spate of cases with an eerily similar plotline: the children of wealthy and powerful elites—often in sports cars—cavalierly violating the rights of average citizens. The meme “my father is mayor!” which one privileged youth was rumored to have said after assaulting a shopkeeper over a parking spot, captured the anxieties and resentment of a highly unequal society.

Online social networking also fueled offline collective action. Thousands of local citizens took to the streets to protest chemical plants that allegedly posed risks to public health. During demonstrations in Dalian (August 2011), Shifang (July 2012), and Ningbo (October 2012) among others, residents flooded microblog sites with
images and descriptions of street marches and battles with police. In contrast, news coverage of these incidents in mainstream media was scant. Perhaps most famous in Western quarters, the Wukan Uprising (September – December 2011) originated when a group of citizens established a Tencent QQ online chat group in 2009 to discuss grievances over land seizures by local officials.

Against this backdrop, Beijing Municipality promulgated provisions on the administration of microblogs in December 2011 (“Beijing Provisions”). These provisions became effective in March 2012. They required users to register their real identity details in order to post or forward content on a microblog. Since two of the main microblogging platforms, Sina and Sohu, were registered in Beijing, they immediately became subject to the real name policy. Following the 18th Party Congress, in late 2012 the Standing Committee of the National People’s Congress passed legislation, giving the real name policy national applicability and the full force of law. The system allows pseudonyms to continue to serve as screen names or handles, but requires users to register with their real name, home address, and national identification number in order to use an online platform’s comment functions.

It is too soon to assess the impact of China’s real name registration system. However, since enactment of the Beijing Provisions in March 2012, enforcement has been spotty. One month prior to the deadline for compliance with the provisions, Sina threatened to suspend anonymous users accounts if they failed to register. Following the deadline, the company prevented anonymous users from utilizing certain social networking functions. However, after a few days Sina restored the original service. On the date the Beijing Provisions became effective, only about 19 million of 300 million Sina Weibo users had registered with their real names.
Soon thereafter, microblog platforms were rocked by the spectacular downfall of Chongqing Party Secretary and potential Politburo Standing Committee appointee Bo Xilai. Online service providers, operating in crisis mode, called on netizens to abide by the law, not forward rumors, and to report individuals spreading rumors.\textsuperscript{61} In response to “lawless elements,” Sina Weibo reportedly closed four user accounts.\textsuperscript{62} Circumstances suggest that Sina provided the personal information of these users to state authorities, and two of the former account holders disappeared as of March 25, 2012.\textsuperscript{63}

The Beijing Provisions could not check the rumors surrounding the imminent leadership transition. One month prior to the Party Congress, in September 2012, online rumors flew after presumptive President Xi Jinping missed a number of meetings with foreign dignitaries.\textsuperscript{64} Speculation ranged from the mundane (Xi pulled a muscle while swimming) to the sensational (Xi was recovering from injuries after an assassination attempt).\textsuperscript{65}

Web users also continued to use online forums to shine a spotlight on local government corruption, a trend dating back at least four years.\textsuperscript{66} In one example, netizens succeeded in triggering the investigation and removal of Shaanxi safety chief Yang Dacai.\textsuperscript{67} The month-long online campaign originated with a tweeted image on Sina Weibo showing Yang smiling at the scene of a horrific accident, which claimed the lives of 36 bus passengers.\textsuperscript{68} Citizen “sleuths” subsequently posted photos of Yang wearing a variety of expensive watches, and the allegations of corruption ensued. The government’s response to netizen allegations directed at higher-level central government officials, however, has lagged.\textsuperscript{69}

Possibly as part of a public relations effort by the incoming Xi administration, mainstream news outlets, including CCP mouthpiece \textit{People's Daily}, seemed to
embrace online anti-corruption efforts. In the months following the 18th Party Congress, official reporting showcased eight city and provincial-level government officials under internal investigation for improprieties and alleged illegal conduct. The reports highlighted the fact that online networks of citizens exposed corruption in a number of these cases. Official coverage paid lip service to the value of citizen whistleblowers. At the same time, the reports noted that “authenticity and accuracy” cannot be guaranteed when coming from an anonymous whistleblower, and efforts must be made to further “systemize” and “standardize” online anti-corruption.

C. Facebook: The Global Behemoth

Facebook presents an interesting contrast to the previous cases because it is a large, transnational network and a NASDAQ-listed public company. There are around 2.5 billion Internet users globally. As of September 2012, more than one billion of them were on Facebook. It has become the most popular social networking service in the vast majority of countries, and now faces tough battles for dominance in a handful of countries with popular local competitors and governments that block the site. While consumers can choose whether to open an account on Facebook or another social networking service, no other service offers the breadth of network internationally and, often, nationally as well.

According to research from the U.S. context, users feel that the ability to create and maintain relationships is the main benefit of Facebook and similar online networks. The creation and preservation of a network based on interpersonal relationships requires the disclosure of private information to a virtually unlimited audience. For this business model to work, users must feel that their private information is secure and trust that the identities of “friends” online are genuine.
Given the massive scope of its network, Facebook has had relative success instituting a real name policy. Users are required to provide their name as it appears on their credit card or student ID. The official policy states: “We remove fake accounts from the site as we find them.” Facebook’s internal estimates reveal that approximately 8.7 percent of all user accounts are fake. As with the sale of followers on China’s microblogs, private companies have engaged in the sale of Facebook “friends.”

Facebook uses technology to track profile behavior and relationships, and when a “fake” profile is found, pages that have links to it are also checked. This is done in the name of safety and security. The removal of everything from fake celebrities to pages representing pets is a regular occurrence. Criticism has hinged on the widening external exposure of users’ personal information to third parties without adequate notice or the ability to opt-out. The private information amassed by Facebook offers opportunities for microtargeted marketing and advertising, particularly when profiles are combined with functions that track user behavior. The demand for this information is the most viable way for the company to monetize its free social networking service. For this reason as much as safety and civility online, real names are essential to Facebook’s business model.

The real name rule has not prevented false impersonation and scams to defraud, fake pages amounting to libel, malicious messages, or trolling. In a 2009 statement, Facebook told CNN that impersonation schemes affected less than 1 percent of the social network’s 150 million users. According to an independent survey of U.S. users, almost 18 percent of respondents reported negative experiences on Facebook, including unwanted advances, stalking, harassment, damaging gossip,
or rumor, or data theft. The social network has mitigated some of its enforcement costs by letting users flag spam and identify inappropriate content.

In incidents across the globe, online networking through Facebook has facilitated political mobilization offline. One example from Hong Kong speaks to the versatility of Facebook as a tool of political organization. Following the Hong Kong chief executive’s endorsement of Moral and National Education (‘MNE’) as a required element of school curricula, student opposition organized around a Facebook page, called “Scholarism,” created by secondary school student Joshua Wong Chi-fung and others. The page garnered more than 150,000 fans and stood at the center of a sophisticated communications campaign. Page content not only informed students of upcoming events and rallies but also, through multimedia features, provided a forum to share touchstone messages and images, such as the image of a blindfolded youth with wrists crossed in an “X,” and the refrain “Hey! Teacher! Leave them kids alone!” from Pink Floyd’s Another Brick in the Wall, which galvanized the movement.

Eleven schools across Hong Kong organized subsidiary Facebook pages affiliated with the Scholarism brand, detailing anti-MNE events specific to that campus. The National Education Parents Concerned Group followed suit with its Facebook page. Allied pages from Hong Kong communities abroad, such as the Vancouver Alliance Against Moral and National Education, sprouted up. The movement culminated in marches of several tens of thousands of protesters, a 10-day sit-in of government headquarters, and hunger strike immediately prior to the September 2012 legislative council election. The day before the election, the government retreated from its earlier position that MNE be mandatory.
Facebook’s adherence to the real name policy has sometimes led to the deletion of profiles and fan pages of political activists. Hostile governments have used the Facebook terms of service against users. A government agent may discover that the administrator of a page uses a pseudonymous account and report this violation to Facebook. In the past, Facebook’s automated servers have responded by immediately shutting down the account. The appeals process to have a closed account reinstated is not well defined.  

In April 2011, Facebook removed dozens of pages challenging U.K. government policies, such as an increase in student fees. The targeted pages utilized fake profiles. While Facebook claimed it was merely adhering to its policy, media commentators suggested Facebook was complicit in a government-directed security crackdown in the lead up to the royal wedding. 

During the revolution in Egypt, Facebook removed the “We are all Khaled Said” page in November 2010 after discovering that the administrator used a pseudonym. The popular page was named in remembrance of an Alexandria man murdered by police. It had become one of Egypt’s most activist sites with more than 400,000 fans. The page sought to coordinate election-monitoring activities in the lead up to parliamentary elections, expected to be heavily-rigged. The page encouraged fans to document illegal and fraudulent election activities, but on Election Day the page was taken down. The case drew the attention of international civil society, including U.S. based Freedom House and the Committee to Protect Journalists, and media. Facebook belatedly allowed a proxy administrator in the U.S. to stand in for the page’s pseudonymous administrator in Egypt and allowed the page back up. The incident drew the attention of the U.S. Congress. Senator Dick Durban and others have named Facebook for not doing enough to protect human rights.
II. Why Real Name Registration Hasn’t Silenced the Citizens of South Korea or China

Both democratic and authoritarian governments have employed real name registration to manage online speech. These governments have tended to frame their real name policies as part of an effort to eliminate bad speech, such as harassment, fraud, or rumor. However, the cases of South Korea, China, and Facebook suggest that real name registration can be part of a strategy to silence dissenting voices. Politicians understandably feel threatened by new media, which has disrupted longstanding messaging and information control mechanisms.

Elections and leadership transitions are particularly sensitive times. Real name registration in South Korea originated in an electoral law; in China the real name law coincided with the succession of the fifth generation of party leadership. In Egypt and elsewhere, government forces seem to have taken advantage of Facebook’s real name policy to shut down pages coordinating election-related activism. Even in liberal democracies, with protections on free speech, governments and law enforcement agencies may be expected to push the envelope in seeking access to Web users’ identities and materials published on social media. For-profit companies, like Facebook (or Sina Weibo) can only be expected to uphold human rights insofar as that furthers their commercial goals.

And yet, real name registration did not silence South Korean or Chinese citizens. While blocked in a handful of countries, Facebook remains a forum for activism in a variety of political contexts across the globe. Real name registration did not prevent the viral spread of rumors about U.S. beef in South Korea or conspiracy theories of a coup in China. Facebook, which seems to have had relatively more success fostering responsible speech online, has also witnessed noteworthy cases of malicious speech. Citizens have still used online forums to organize offline collective
action. So it seems the border into Orwellian dystopia has not yet been crossed. The analysis below explores why real name policies are so difficult to carry out by examining incentives of online service providers and citizens.

A. The Perspectives of Online Service Providers

An online real name registration system is costly. It requires human administrators, and technical safeguards to protect the personal information of users. First, there is the administrative burden of verifying whether the identification details of each account are genuine. A thriving industry offering fake identities, and allowing Web users to pump up their online popularity through the purchase of “zombie” followers or friends, further aggravates the burden.

There are also information security concerns. In an addition to the hacking of 35 million Cyworld accounts in South Korea, hackers disclosed the personal account information of more than 6 million users from China Software Developer Network, China’s largest online community for programmers in 2011. Since Facebook does not require that users provide personal identification numbers, it does not present an opportunity for the same kind of identity theft. Nevertheless, Facebook collects a substantial amount of private data, and Facebook systems have been subject to sophisticated hacking attacks. If online service providers vigorously enforce the real name policy, users’ fears that their personal information may be hacked could prove a deterrent to their continued use.

Online service providers bear the bulk of these costs. Their willingness and ability to enforce a real name policy varies based on a complex set of incentives. In the context of a legal mandate for real name registration, as in South Korea and China, service providers have a commercial incentive to enforce the real name policy, or else risk punishment. But the threat of fines or shut down can lack credibility.
Governments may view online service providers as strategic partners, or they may be reluctant to censure these revenue-generating business entities. One month prior to the deadline, Sina attempted to enforce the 2011 Beijing Provisions by threatening to suspend anonymous users accounts. Following the deadline, the company prevented anonymous users from utilizing certain social networking functions. After a few days, however, Sina restored the original service, and government authorities apparently allowed it.  

Service providers’ willingness to enforce a real name policy also depends on their market position. China has blocked foreign social media platforms from accessing its market, opening the door for domestic “clones,” such as Renren (for Facebook) and Sina Weibo (for Twitter). Shielded from foreign competition, Chinese social networking service platforms have proliferated, and the sector is heavily fragmented.

Service providers face a “prisoners dilemma,” where each has an incentive to shirk its enforcement responsibilities. Weeding out anonymous users could negatively affect content or a social media network’s brand in the eyes of Web users. Service providers may worry that enforcement of the real name policy will cause them to lose market share. A provider has an incentive to drag its feet in enforcement. If a competitor enforces the law first, the provider may capture some of that competitor’s market share. The result is inaction and general reluctance to enforce the policy across the board.

In South Korea, regulators decided not to subject foreign Internet service providers to the real name registration law. The Korean Constitutional Court found that, during the period the law was in effect, the number of Korean users of foreign online service platforms increased, and Korean companies created domains in foreign
jurisdictions. The threat of losing market share to foreign competition unified an influential domestic constituency against the real name registration law.

Facebook enjoys the advantage of having consolidated a dominant position in key national markets early in the game. Now, the breadth of Facebook’s transnational network allows it to offer a relatively unique service. Some competitors, such as Google+, have tried to poach Facebook users. Google+ has sought to differentiate itself with a (marginally) softer real name policy, but Google+ still trails far behind Facebook in terms of market share.

The nature of the particular social media service also affects a provider’s propensity to enforce a real name policy. Some services are more socially driven while others are more content driven. Generally, socially driven platforms are designed to facilitate interpersonal connections and friendships. In this context, users place a premium on knowing their online counterparts’ true identities. On the other hand, users of content driven services are more concerned with what is being said rather than who is saying it.

Service providers such as Facebook have an easier time getting users to comply with real name policies than more content driven platforms like microblogs. At one end of the spectrum, instant messaging services like WhatsApp or Weixin are examples of highly socially driven platforms. They allow users to access their network of mobile phone address book contacts. Their service is about communicating with existing friends. Facebook, Cyworld, and Renren are also examples of socially driven network services although slightly less so. On these platforms, users are sharing and consuming a more content, which can be a very personal form of self-expression. Microblogs like Twitter and Sina Weibo are still more content driven. Users check their accounts for breaking news, gossip, as well as
personal developments. While this genre of information used to be the province of professional journalists, anonymity liberates the average citizen to join the discussion in real time. Pseudonymously generated content may be precisely the sort of juicy tidbits that users have signed on to see.

**B. The Perspectives of Citizens**

For citizens living in areas with Internet penetration like South Korea or China’s more developed municipalities, life without online social interaction is almost unthinkable. Social media has deeply penetrated users’ everyday lives and, as pervasive technology, has become expected and even taken for granted. Studies have shown that Web users derive intense psychological gratification from social media. This is particularly captured in stories of college-age Web users that return to Facebook even after suffering repeated humiliations of having their profiles hacked and manipulated.\(^\text{107}\)

The ability to connect to a broader network is meaningful to people because it affirms their individual dignity. Minorities and people with unconventional views can see that they are not alone. For example, the website aibai.cn has become one of the best known Chinese language websites dedicated to the LGBT community with more than 55,000 daily visits.\(^\text{108}\) The website offers several advice columns, including a legal advice question and answer page. In societies where governments have restricted traditional media, online social media offers netizens a particularly eye-opening and unique atmosphere. The knowledge personally targeted monitoring and surveillance that comes with real name registration diminishes this liberating experience. The imposition of real name registration affects wired societies broadly, far beyond the relatively small population that rely upon online anonymity to express themselves.
C. More Trouble Than It’s Worth?

Netizens will resist state efforts to restrict their freedom of expression through real name registration. Given the gratification experienced as a result anonymous speech online, the threat of punishment will need to be certain and harsh in order to motivate people to reregister. But these levels of enforcement are unlikely. Online service providers prefer not to shoulder the additional Web development, monitoring, and security costs. Factors, such as market fragmentation and the nature of the social media service, may negatively affect enforceability. Where the market is fragmented, service providers have an incentive to foot-drag. For more content driven social media, such as microblogs, eliminating pseudonymous accounts may degrade content and depress site visits.

At the same time, governments are becoming more social media savvy, establishing their own channels for online communication with citizens. With China’s online anti-corruption experiment, for example, the central government seems to be testing the proposition whether citizens who can speak out will choose not to act out. In the end, governments may determine that real name registration is more trouble than it is worth.

---

1 David Caragliano is a senior program officer at the National Democratic Institute for International Affairs in Washington, DC. Previously, he practiced law at an international law firm in Hong Kong. Please direct questions and comments to: DCaragliano@ndi.org.


5 Id. at 353


7 Supra, note 4 at 358.

8 Public Official Election Act, art. 82, provision 6. See also Freedom House Report.

9 Id.


13 Id.


16 Id. See also Byongil Oh, Global Information Society Watch: Republic of Korea, Korean Progressive Network Jinbonet (2010), www.jinbo.net.


18 Id.


21 Id.

22 Supra, note 19.

23 Id.

25 Supra, note 20.

26 Id.


29 Supra note 20.

30 Id.

31 Id.


34 Supra note 4.

35 Id.

36 Id.

37 Id.


40 Korean Constitutional Court Decision.

41 Id.


44 Id.

45 *China’s Internet Base to Hit 800 million by 2015*, MARBRIDGE DAILY, Jan. 6, 2013.


Information Protection Law, art. 6.


Id.

Id.

Id.

Id.

Id.

Id.

Id.

Id.

Id.
Bernhard Debatin et al., *Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences*, 15 J. OF COMPUTER MEDIATED COMMUNICATIONS 83, 87 (2009) [hereinafter “Facebook Study”].

Id.

Id.

Id.

Id.


Supra note 83.

Facebook Study at 93.


https://www.facebook.com/parentsconcerngroup?group_id=0.


Supra, note 3.

Supra, note 82.

Id.

Id.

Supra note 3.


Korean Constitutional Court Decision.


Facebook Study at 101.