BE PREPARED

READY OR NOT

A clear strategy for handling a data breach can spare companies a lot of pain, says Brunswick's GEORGE LITTLE

Companies that have clear plans in place to handle data security breaches fare better than those that don't. Some of the largest breaches ever reported, including those suffered by five Fortune 500 companies, are analyzed in the chart below. Those that were better prepared responded more effectively, according to an analysis by AllClear ID, which specializes in data breach preparation and response.

The letters A through H reflect the combination of preparedness and effective response to a breach – each combination may be common to more than one company. Preparedness was measured by factors such as the level of detail in a response plan; the establishment, in advance, of a "war room" of personnel to handle a crisis; and at what point outside experts were brought in to assist. Response effectiveness was measured by factors including media coverage, expenses and how well the communications team managed.

Execution proves to be a critical factor. In scenarios B and C, companies' responses scored highly, in spite of above average but less than perfect preparation. Meanwhile in D, companies scored lower for response effectiveness, despite their preparation, due to poor decision-making during the response.

FAILURE TO PLAN IS A PLAN TO FAIL

Preparation and outcome

A Had a detailed incident response plan in place prior to the breach, and a smooth response
B Took timely advice from experts, allowing a better response
C Had experience in breach response, strong operational capabilities and executive support
D Waited too long to release information, which resulted in damage from outside speculation
E Disorganized response led to delays and communications problems
F Lack of executive support and poor decision-making increased expenses
G Lack of a centralized decision-maker led to confusion, delays and disruption
H Lack of preparation led to communications missteps, poor decisions and poor customer support

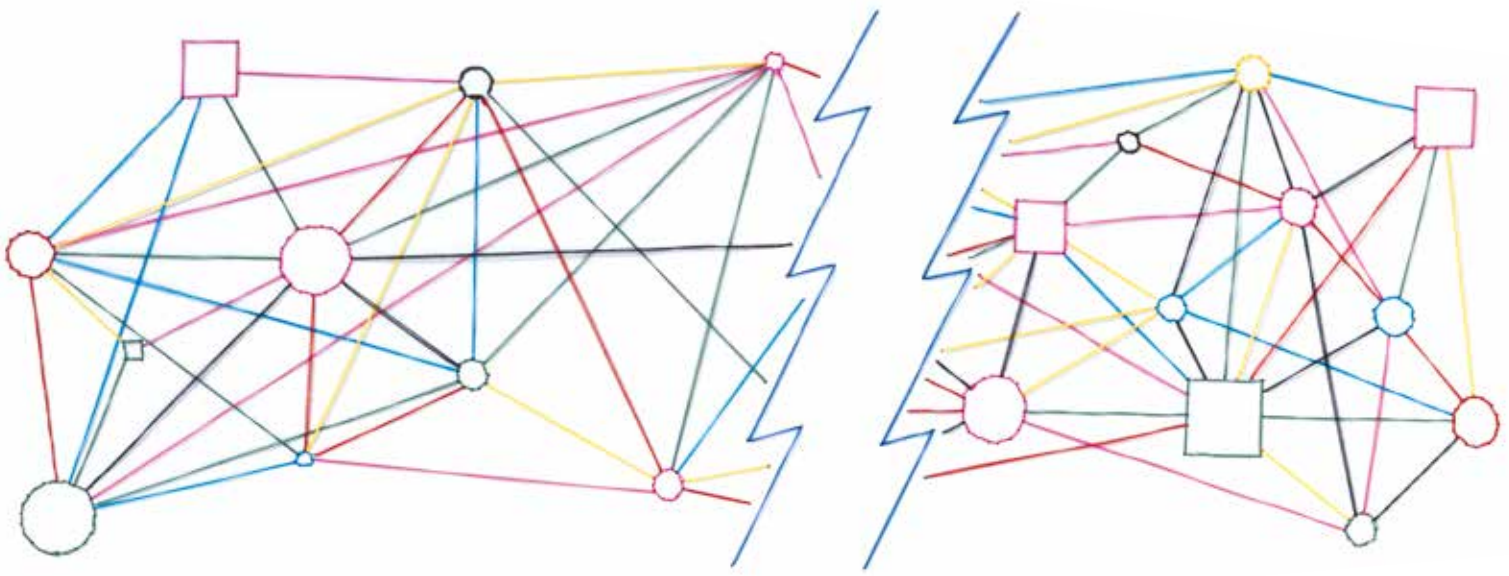
SOURCE: ALLCLEAR ID

When the Berlin Wall fell in 1989, the well-respected forecasting firm Global Business Network was asked to develop scenarios for the emerging world order. GBN offered three. The first was Change Without Progress, a kind of high-tech gangster capitalism familiar to some oligarchs today. Second, New Empires outlined a nationalist or regional neo-mercantilism. The third, Market World, anticipated a fast-paced, globally integrated finance capitalism.

History has unfolded according to the third option. We are living in a global marketplace where investments and information flow more or less freely across national borders. The globalization of data along with open internet access has increasingly provided a common highway for this Market World. But national interests and the defense of citizens' privacy are now pushing hard to roll back that scenario toward something closer to the New Empires by curbing the free flow of information across borders. Again, as in 1989, the world is changing – only this time, walls are going up.

SINCE THE REVELATORY US government leaks by Edward Snowden, countries including Brazil, Germany and India have publicly discussed their desire for greater data protection and national, protected internets. The idea of the global internet devolving into a constellation of national networks has been called the "splinternet."

American Ambassador Michael Froman, head of the Office of the US Trade Representative, describes this trend as "an accelerated rise of 'data nationalism' and a digital world that begins to erect barriers rather than transcend them." German Chancellor Angela Merkel recently promised, "We'll talk about European providers that offer security for our citizens, so that one shouldn't have to send emails and other information across the Atlantic." The EU and Brazil have already announced their intention to install a $185 million



DATA NATIONALISM

THE RISE OF THE "SPLINTERNET"

The backlash from privacy breaches could change the internet as we know it, says Brunswick's ROBERT MORAN

underwater fiber-optic cable that bypasses the US. Splinternet 1.0 may have arrived.

How any of this could work in practice is anyone's guess, given the unstoppable, exponential increase in data from internet-connected devices, products and services. But the splintering trend is likely to grow, complicating the international business landscape.

Data is a hot commodity. To the individual, consumer data is either a resource or a part of their person, a kind of third skin, after the dermis and clothing. An Ipsos Global Trends survey of 20 countries found that 60 percent of people are concerned about how their data is being used. Reflecting that concern, governments are examining how the privacy rights of their citizens can be better protected.

However, data can also be viewed as a natural resource, like oil. For nations, this means data collection and analytics, servers and transmission lines are as integral to economic interests as offshore wells, refineries and tankers. Sir Walter Raleigh famously asserted, "Whosoever commands the sea commands the trade; whosoever commands the trade of the world commands the riches of the world and consequently the world itself." The control of data delivery systems is the modern equivalent.

Andrew Marshall, the influential 93-year-old military futurist often referred to as "Yoda" in American defense circles, espouses a theory known as Revolution in Military Affairs, the modern corollary to Sir Walter Raleigh's view. The theory holds that each weaponized technology leads to a new kind of warfare. The first to master the technology gains the upper hand. Chariots, iron, gunpowder, steam power, rifling, air power, atomic weapons, precision munitions and robotics each reinforced the dominance of the wielding parties.

For nations ... data collection and analytics, servers and transmission lines are as integral to economic interests as offshore wells, refineries and tankers

If data and information transmission are the next leap, the first-mover advantage would lie in cyberwarfare and computer viruses such as Stuxnet, a software worm said to have severely damaged Iran's nuclear program in 2011. Recognizing this, former National Security Agency and CIA director Michael Hayden likened America's policy toward the internet to the Roman roads that supported both an explosion of trade in the ancient world and the mobility of the Roman army. Rome built the roads and also patrolled them, making them safe for commerce while expanding the empire's authority. Similarly, the US protects American interests through data channels, prompting Hayden's observation that the US "could be fairly charged with the militarization of the World Wide Web."

DATA NATIONALISM is a natural outgrowth of that thinking and is already coloring relations between countries and regions. In Brunswick's polling among Washington elites, "data privacy" was flagged along with "food safety" as one →

of the top two issues that could be difficult for the US and the EU to reach an agreement over in trade negotiations. Could data nationalism slow growth in the global trade of digital goods and services as well as knowledge exchange? Common sense suggests it could.

The issue of national identity alone could prove an obstacle. Governments will likely favor locally based corporations and form policies that will tilt the playing field to their advantage. But such measures are a double-edged sword, making international competition more complicated. Governments are also more likely to expect special favors from those domestically rooted companies.

As more corporations globalize and virtually every one becomes a data company, they will be navigating a world where data nationalism guides policies, and requires the development of nation-specific strategies. Here are some ways that this new breed of nationalism will impact your business:

- Competing policy views between nations over the rights to use consumer data will force the development of many alternative ways of collecting and handling data.
- Compliance handling will grow much more complex and expensive.
- National affiliations will play a much larger role, for better and worse. Businesses may benefit from the policies of their home governments, but also be expected to support domestic interests.
- Some companies may benefit from the rise of data nationalism, supported by national or regional barriers that put stronger international competitors at a disadvantage.
- Communications will be even more critical, as all stakeholders in all markets will want to know a corporation's data strategy. Businesses will need to show how their policies are a win for shareholders, customers and governments in each and every country in which they do business.

ROBERT MORAN leads Brunswick Insight, the group's global public opinion research function, and is a Partner in the Washington, DC office.

REGULATION

Business can avoid a fragmented global landscape on data regulation by speaking up, say Brunswick's MARK SEIFERT and KATE TELLIER

The more business remains on the sidelines in the public conversation over the use of data, the more global policymakers will take the lead, tackling ethical questions surrounding data collection, privacy and security.

Political leaders want to see data used for innovation to drive economic gains, support industries and improve social services, but they are also moving to respond to citizens' concerns. "As businesses navigate the digital world, there is no more fundamental issue to address than protecting their customers' privacy," says Nuala O'Connor, CEO of the Center for Democracy and Technology, an international non-profit promoting an open, innovative and free internet. Many businesses are making great efforts to protect their data, but communication about those efforts has been spotty at best.

More importantly, the positive potential of data needs to be emphasized to address growing public anxiety. Ultimately, data collection and analysis could serve to change our nature as a species as fundamentally as the harnessing of fire. If the perception of value is obscured by public concerns, which are growing around the world, that transformation could be snuffed out.

IN THE EUROPEAN UNION, the future of data is being factored into plans for continued economic recovery. While some proposals would make online business easier by simplifying

laws, negotiations around others, such as the Transatlantic Trade and Investment Partnership with the US, have triggered data protectionism based on privacy concerns, with the potential to restrict international data flows. Similarly, in an idea modeled on the Schengen zone – where most of Europe functions as a single country for international travel purposes – data coming in and out of Europe would be restricted, while internal traffic would not.

In the US, the Republican-controlled Congress is set to take a pro-business, decidedly deregulatory approach. That effort could face a strong challenge from Democrats as the Obama administration, now in its final two years, is willing to assert executive power to institute greater regulatory scrutiny. The White House recently appointed its first chief data scientist to ensure that national data is not misused and to investigate ways to help people share information without sacrificing privacy. Headed into the presidential election in 2016, both parties will attempt to present a balance between consumers' privacy concerns and the transformative potential of data analytics.

> "Our ethical stance, if my data is blood – if it's going to save lives – is different than if my data is of a sort that can be ethically monetized"
>
> **Robert Madelin, EC Director-General of Communications and Technology**

"In this new Congress, I will be focusing on a pro-innovation technology agenda that relies heavily on an open internet," says Republican Senator Orrin Hatch of Utah. "In particular, we must address the complex legal web around data security, including the ways data is used, stored and accessed globally."

Senator Ed Markey, a Democrat for Massachusetts, says, "Consumers, not corporations, should have control over their personal information in this era of Big Data. Whether it is protecting our children's education records or the sensitive information of American consumers, Congress needs to ensure that our policies are imbued with our time-tested privacy values."

South America is leaning toward an EU-style precautionary approach that favors domestic companies. A provision mandating data localization in Brazil's recently enacted *Marco Civil da Internet*, a civil rights framework, would have been aggressively nationalist, but was removed from the final version.

Most major economic centers in Asia have enacted privacy legislation but enforcement is in its infancy. In addition, regulators in emerging economies are exploring appropriate responses that avoid pitfalls experienced in the EU and the US.

Many of the EU initiatives to restrict the use of data stem from misperceptions about what companies actually do with data and how this contributes to society. →

A clearer narrative from business, including an emphasis on the critical distinction between personal and non-personal information, could help loosen this regulatory knot and raise confidence in the positive impact of data.

"I like to think of data as having value, but it might be oil or it might be blood," says Robert Madelin, Director-General of Communications Networks, Content and Technology for the European Commission. "Our ethical stance, if my data is blood – if it's going to save lives – is different than if my data is of a sort that can be ethically monetized."

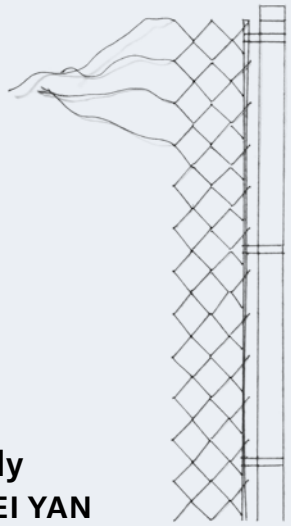
SCANNING the global landscape, we appear headed toward a discordant set of rules that could result in the fracturing of the internet, undermining its power as a global, equal-access knowledge base. A heavily pro-business argument that ignores consumer concerns could inadvertently strengthen support for nationalist regulatory tendencies.

So what should companies do, especially multinationals, within this regulatory patchwork? In a word: engage.

Most companies understand the power of data analytics for their business. They should also recognize the threat of regionally based regulation. By getting ahead of consumer and government concerns, companies can move toward a more nuanced conversation about how data is being handled and the power of analytics to change society for the better. Multinational companies are best positioned to make this case, thinking globally and responding locally.

Unleashing the digital revolution in a controlled environment could bring unimaginable benefits. Businesses should start to tell that story, before overly stringent regulation hijacks the narrative.

MARK SEIFERT is a Partner in Brunswick's Washington, DC office, advising on corporate data, privacy and cybersecurity.
KATE TELLIER is a Director in Brunswick's Brussels office and advises on European public affairs related to the digital economy.
Additional reporting by **MATHILDE BONNEAU**, Account Director in Brussels.



CHINA

EVOLUTION OF PRIVACY

Until recently, the concept simply didn't exist, says Brunswick's MEI YAN

For centuries in China, ruling powers advocated for social responsibility and cohesion, and treated individuality with suspicion. Until fairly recently, the concept of privacy, as the West understands it, simply didn't exist.

This absence is most clearly evident in the Chinese language. Until the 20th century, the language lacked a word for "privacy" or even the vocabulary needed to communicate the concept. The compound that eventually emerged, "yinsi"(隐私), has negative connotations of secrecy and conspiracy, as does the phonetically similar word for "hell" – "yinsi" (阴司).

The Mao era reinforced this vice-over-virtue view of privacy with the glorification of collectivism. From the very foundation of a society built on public ownership, to the treatment of individual lives as an open book, lack of privacy was the norm, reinforced by Communist Party monitoring even at the grassroots "neighborhood committee" level (居民委员会). Private thoughts showed selfishness and brought shame, persecution or worse.

The negative framing of privacy was upended by China's "open door" policy. Launched in 1978, it ushered in economic reforms that eventually enabled private and individual ownership. The Party's shift set off a major social evolution, paving the way to greater acceptance of personal privacy.

As a backlash to China's collectivist past, in the post-reform era people have begun to see individual privacy as a right that should be guarded and respected. Yet the concept is still very much in flux, with the internet and the widespread adoption of social media playing important roles.

In China, the internet has sparked a mass invasion of privacy known as "human flesh search engines" – digital witch hunts by netizens nationwide who band together to identify and shame individuals perceived as having violated public morality. While the trend is often seen as a positive force to root out socially unacceptable behavior, it also intrudes deep into private lives.

Early examples of people who had their names, addresses and other private details exposed on the internet include a woman who complained that coverage of the deadly 2008 Chengdu earthquake was disrupting her TV viewing. Another notable case is that of "Uncle Watch," a government official who was outed by online vigilantes for flaunting multiple luxury watches while attending official duties.

"Yinsi" may no longer be closely associated with "hell," but these incidents highlight how the concept is still evolving. Ultimately, respect for personal privacy in China is destined to become more natural, as people begin to appreciate privacy as a daily necessity rather than a luxury.

MEI YAN is a Senior Partner in Brunswick's Beijing office. She advises major global corporations, with a particular focus on public affairs. As a journalist for *ITN* and *CNN*, she was a three-time Emmy winner.