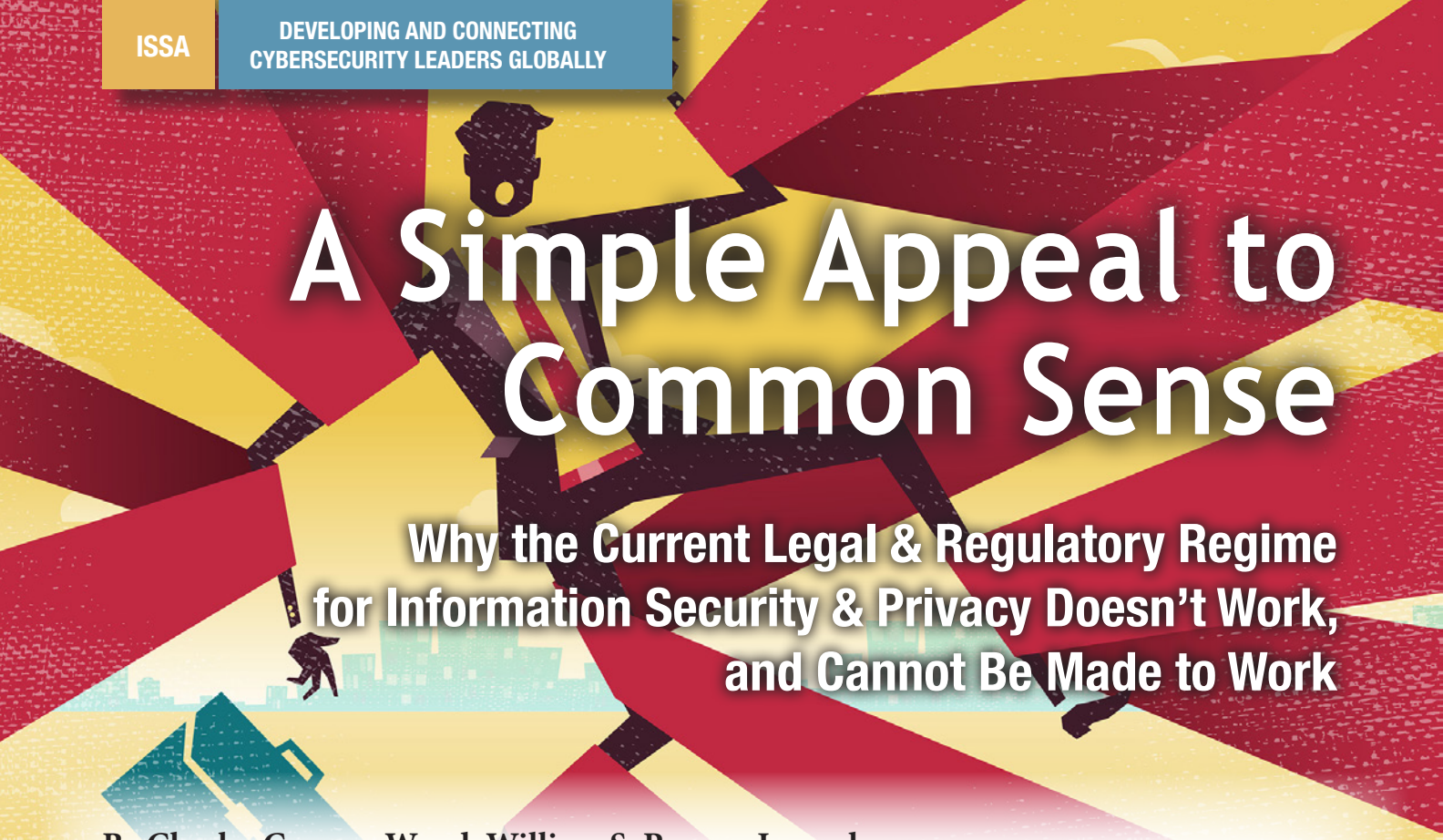

A Simple Appeal to Common Sense

Why the Current Legal & Regulatory Regime for Information Security & Privacy Doesn't Work, and Cannot Be Made to Work

By Charles Cresson Wood, William S. Rogers, Jr., and Ralph Spencer Poore – ISSA Distinguish Fellow, North Texas Chapter

This article explores nine specific reasons why the current legal and regulatory process doesn't work and cannot be made to work, and why a new and radically redesigned process is now required.

Abstract

This article is an appeal to common sense, asking those working in the information security and privacy field to pause, reflect, and get out in front of the rapidly moving train long enough to lay some new track, to go in a different direction, a direction that has some hope of being successful in the years to come. If readers step back and objectively consider the current landscape of information security and privacy laws and regulations, it quickly becomes clear that the process now employed does not work. Worse yet, no amount of changes to the inputs to the existing process (more people, increased salaries, more training, increased budgets, new technology products, etc.) can make that same process work efficiently and effectively.

This article explores nine specific reasons why the current legal and regulatory process doesn't work, and cannot be made to work, and why a new and radically redesigned process is now required. Those nine reasons can be summed up by the assertion that the present process is too slow, too inflexible, and too nonresponsive (unable to evolve and adapt) to adequately meet to the true needs that we face today. The article is not normative in the sense that it proposes a particular new way to do things. Instead, the article is simply calling for a convention or similar multi-party harmonization effort to seriously investigate how we might design a new legal and regulatory process that has a grounded hope of being both effective and efficient.

Recent events provide ample examples of the dramatic and serious damage done by failures associated with the current information security and privacy rule-making system. Consider that the software VW developed to defeat smog emissions testing, arguably a computer crime of multi-national proportions, went undetected for six years.[1] On another note, a large region in the Ukraine with 230,000 affected people was plunged into an electrical blackout via a sophisticated power grid sabotage attack perpetrated by hackers, an attack that not only disabled the existing

1 Bruce Schneier, "VW Scandal Could Just Be the beginning," CNN Opinion (September 28, 2015), http://www.cnn.com/2015/09/28/opinions/schneier-vw-cheating-software/.

grid but grid back-up systems as well.[2] And also consider, as a further data point, that a nation state (allegedly North Korea) attacked a major corporation (Sony Pictures). The latter attack was so devastating to information security and privacy systems that management at the victimized firm was left communicating only with traditional land line telephone systems and paper memos.[3] While many other recent examples could be cited, it is clear that current information security and privacy losses are spiraling out of control, and the applicable laws and regulations, and the supporting infrastructure (such as police) is collectively failing to control these mounting and often devastating losses.

Why the existing legal and regulatory system doesn't work

1. Jurisdictional fragmentation creates confusion, unnecessary costs, and lack of action

The traditional and still-prevailing jurisdiction-by-jurisdiction approach, even when partially-unified such as it is with the European Union in the domain of privacy, is not practical in a world interconnected by the Internet. The Internet erases national boundaries and connects both individuals and organizations much more tightly than was ever previously possible. At the same time, the complexity and multi-layered nature of software provides new and powerful methods to conceal both the location and the identity of the parties involved in a certain process (encryption being one of the primary methods, but there are many others like bots and virtual reality avatars).

Cloud service providers, furthermore, may store data in one jurisdiction or another, and the ability to move data from one location to another is an important attribute of load balancing, performance management, and contingency planning. If the location and the identity of the parties involved cannot be clearly determined, and if the data's location cannot clearly be determined either, then a regime based on national (or regional) laws and regulations cannot realistically and successfully be applied. What is needed instead is a worldwide legal and regulatory system because the Internet is now also worldwide. Such a new system must include consistent legal and regulatory definitions, as well as consistent enforcement mechanisms such as extradition treaties, search warrants, courts, alternative dispute resolution forums, and electronic discovery processes.

2. Information explosion overwhelms existing decision-making systems

The volume of information created, processed, stored, and now employed in decision-making is increasing at an exponential rate.[4] In part, this explosion is brought about by ubiquitous, powerful, and low-cost new information technology. This explosion is also brought about by increasing world population and the globalization of trade. The Internet furthermore facilitates this explosion because it provides a new and increasing connectivity, as is evidenced by the rapidly-evolving Internet of things (IoT).

A legal and regulatory system based on making decisions on a manual, case-by-case basis may have been sufficient to deal

2 L. Todd Wood, "Ukraine: Russia Hacks Power Plants, Highlights U.S. Weakness," The Washington Times (Dec. 30, 2015), http://www.washingtontimes.com/news/2015/dec/30/l-todd-wood-ukraine-russia-hacking-power-plants-hi/.

3 Lori Grisham, "Timeline: North Korea and the Sony Pictures Hack," USA Today (Jan. 5, 2015), http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645.

4 Gil Press, "A Short History of Big Data," Forbes (May 9, 2013), https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/ - 1225381265a1.

with relatively-simple old-fashioned problems, but it is rapidly overwhelmed by the new complexity and the sheer volume of new situations presented by this information explosion.[5] New approaches that categorize events and situations according to certain pre-determined criteria, and that make dispute resolution decisions uniformly and automatically, must instead be developed, and those approaches must be widely deployed using the latest tools such as artificial intelligence.[6]

The foundational philosophy of laws and regulations must in large measure shift from a reactive focus on recovery, correction, and damages awarded to harmed parties, to a proactive focus on prevention, detection, deterrence, and avoidance.

An impressive array of new high-tech tools can be used to deal with this information explosion by expediting and automating the application of laws and regulations in the information security and privacy domain. These new tools include smart contracts (automatically enforces a contract via software processes), digital signatures (validates that a certain party agreed to be bound by a contract), and block chain encryption (creates a log of legally significant events that cannot be altered).

3. Pace of rule changes cannot catch up with technological change

The traditional rule-making systems used for information security and privacy involve checks and balances, review procedures, and formal approval. For example, at the United States federal level, the legislative process is extremely time-consuming. Delay is an inherent part of the process, as bills are proposed by congressional committee, hearings are held, and then both the House and the Senate must deliberate, debate, and then vote. Then a signing from the president must take place—all of this taking place only once in the most-expedited of scenarios—but still no implementation of the new rule has occurred.

It may be months or even years later before actual changes in rules for enforcement are implemented (often following separate public hearings). All of this is far too slow in the modern age of high-technology, and this slow-as-molasses rule-making process just further distances the relevance of existing laws and regulations from the new advances rapidly made in technology. We see this large gap between the legal regime now in place and the legal regime that is now needed, for example, in the area of drones, small unmanned flying machines. Not only is a great deal of the law in the drone area unclear (for example, what constitutes a trespass), but the world's leading drone maker is based in China (presenting a potential national defense issue).[7]

4. Waiting for crisis to prompt a new rule no longer works

In addition to the inefficient legislative process mentioned above, United States legal and regulatory rule making often follows decisions by the courts. The latter is slow to evolve by the rule of *Stare Decisis*, or the rule of precedent, as the courts gradually adjust the legal and regulatory approach so as to better fit the situations encountered by litigants. Both the legislative and adjudicatory approaches suffer from the grave fault that they wait for serious crises, like Fukushima (but even that ecological disaster doesn't seem to have prompted much action), before legal and regulatory action is undertaken.

In the domain of information security and privacy, we must instead be proactive. We must anticipate what will happen, and we must take steps to prevent these adverse events from taking place, or at least prepare ourselves to best deal with the adverse effects caused thereby. For example, we should not wait until critical components of our essential infrastructure are destroyed (such as the electrical grid) before we decide that we will undertake more serious protective measures.

Thus, the foundational philosophy of laws and regulations must in large measure shift from a reactive focus on recovery, correction, and damages awarded to harmed parties, to a proactive focus on prevention, detection, deterrence, and avoidance. The widespread utilization of zero-day exploits (unpublicized vulnerabilities for which there are no vendor patches) by both national government intelligence services and organized criminal syndicates further points to the need for this foundational philosophical shift supporting more rapidly evolving proactive laws and regulations.

5. Excessive political and special interest influence prevents adoption of new rules

In too many governments, including the United States, the rule-making process is unduly influenced by ideological political considerations and special interest lobbying groups.[8] Fighting between these groups can, and often does, mean that important information security and privacy decisions are postponed needlessly, and resources are consumed in unproductive ways.[9]

While the authors are not advocating a dictatorial centralized approach, the new rule-making process needs to be expedited

5 "The Overwhelming Impact on the Legal System Is in Evidence at the Patent and Trademark Office (PTO) of the US Government." See Warren K. Mabley, Jr., Deconstructing the Patent Application Backlog, 92 J. Patent & Trademark Off. Soc'y 208 (2010).

6 PTI, Daily News and Analysis, New AI system beats legal practitioners at predicting court decisions, May 8, 2017, http://www.dnaindia.com/scitech/report-new-ai-system-beats-humans-at-predicting-court-outcomes-2430855.

7 Heather Kelly, "Your Guide to Obeying the New Drone Laws," CNN Tech, December 25, 2015, http://money.cnn.com/2015/12/24/technology/drone-faa-laws-registration/index.html.

8 Mike Lofgren, *The Shadow State: The Fall of the Constitution and the Rise of Shadow Government*, 2016, Penguin Books.

9 Consider the way that the Barack Obama Administration reversed the established government information disclosure policies of the George W. Bush Administration and then went on to reverse its own policies. See Reynolds, Maura, "Open Government or Transparency Theater?" http://www.nbcnews.com/id/32128642/ns/politics-cq_politics/t/open-government-or-transparency-theater/ - .WhS6Z7aZPWY, dated July 24, 2009.

and focused solely on important issues, not party politics, not power-grabbing diversions of the rule-making process, and not other delaying side-issues. These delaying mechanisms often sideline or stifle important changes, changes that are desperately needed in order to bring about an adequate level of information security and privacy.

A good example involves user-chosen fixed passwords, which should have been phased out decades ago but are still widely used today. The 2016 Verizon breach report indicates that fully 63 percent of breaches are attributable to antiquated fixed-password technology.[10] Both vendors and users have resisted upgrading their systems to extended user authentication technologies, like multi-factor user access control, which is more secure than user-chosen fixed passwords, because those adopting these new technologies would then be forced to incur large additional costs.

Significantly more emphasis needs to be placed on management due diligence and the immediate needs of technological fixes, and significantly less emphasis needs to be placed on political parties and other special interest considerations. Many of the steps now performed by legislatures and regulators could instead be delegated to a special-purpose organization devoted to information security and privacy rule making. Even within such a special-purpose organization, many tasks could be performed by artificial intelligence, scripted in code, and built into automatically-executing contingency plans.

10 Mor Aduvia, "Verizon DBIR Report: 63% of Breaches Exploit Static Passwords," May 10, 2016, https://blog.gemalto.com/security/2016/05/10/verizon-dbir-report-63-breaches-exploit-static-passwords/.

6. Widespread incompatibilities, errors, and gaps present an attractive attack surface

Research performed at SRI International (formerly Stanford Research Institute)[11] indicates that attackers consistently exploit the gaps, errors, and inconsistencies associated with interfaces between information systems. It is interfaces, and the differences between the involved systems found at those interfaces, that introduce the most attractive opportunities for information security and privacy exploits.[12]

The country-by-country approach to information security and privacy that now prevails (or still worse, the state-within-country-by-state-within-country approach, found in certain areas like US breach notification) presents a very attractive attack surface to perpetrators because it is rife with gaps, errors, and inconsistencies. For example, digital copyright infringement gravitates to those jurisdictions that do not seriously enforce copyright laws.[13]

To overcome these problems, a consistent and unified approach must be established, and that standard of due care must be consistently observed worldwide. To fail to adopt

11 This research was managed by Donn B. Parker, funded by the National Science Foundation, and involved evaluation of reported computer crime and abuse cases.

12 Consider the disastrous oil spill that took place in 1967 off the coast of Cornwall, England. In that event an oil tanker ran into a reef because there was confusion about whether the automatic steering system was enabled, or whether the manual steering system was enabled. Today's systems, for both oil exploration and transportation as well as computer and networking systems, are much more complex than they were back then, and this complexity introduces many more incompatibilities, errors, and gaps that may be exploited. See Tainter, Joseph A., and Tadeusz W. Patzek, *Drilling Down: The Gulf Oil Debate and Our Energy Dilemma*, Springer Science Books, pp. 209-210 (2012).

13 Marc D. Goodman and Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, 2002 UCLA J. L. & Tech. 3 (2002).

such an approach is to invite exploitation by hackers, political activists, high-tech criminals, terrorists, and anarchists.

7. The economics of information security and privacy does not generate, or naturally evolve toward, a self-healing marketplace

Competition among vendors of high-tech systems now encourages fragmentation of the marketplace (for example, via systems that are incompatible with those of other vendors) in order to achieve vendor-specific competitive advantage. This fragmentation further exacerbates the problem mentioned in the prior paragraph, involving an attractive attack surface. For instance, nearly a billion users have been left exposed when vendors refused to upgrade the operating systems in their smart phones.[14]

Furthermore, top management at corporations are currently incentivized by the prevailing accounting and financial system to minimize costs and maximize revenue in order to receive quarterly bonuses, promotions, increases in the price per share, etc. Top management is not sufficiently incentivized to invest in the development of the technological and organizational infrastructure necessary in order to provide adequate information security and privacy.

The fact that current economic incentives are working to the detriment of information security and privacy is illustrated by the massive new fines that can be imposed by the latest version of the European Union's General Data Protection Regulation (2016). That these regulators are now able to fine organizations up to four percent of worldwide annual turnover speaks to a certain level of frustration, a certain level of having to make fines draconian in order to get top management's attention.[15]

Current economic incentive systems associated with information security and privacy are in desperate need of alignment with management incentives,[16] and this alignment can be achieved in part via a new worldwide rule-making process. This article takes no political position regarding the best economic system that encourages appropriate decisions (capitalism, communism, socialism, etc.), asserting only that the current legal and regulatory regime is clearly not working and that we urgently need a new and better approach.

8. Relative investment differential between protectors and attackers will only widen

The research and development investment of high-tech firms, as well as the comparable research and development investment of attackers such as organized crime syndicates and government spy agencies, collectively now far outstrips the comparable investment being made by all groups making and enforcing relevant laws and regulations. In the future, we can expect that the investment of this first collective group—those creating vulnerabilities via introducing new technological innovations and those discovering how to exploit those new vulnerabilities—will continue to dominate and far overshadow the investment made by groups involved in making and enforcing the laws and regulations.

14 Joel Hruska, "Google Throws Nearly a Billion Android Users Under the Bus, Refuses to Patch OS Vulnerability," Extreme Tech, January 12, 2015, https://www.extremetech.com/mobile/197346-google-throws-nearly-a-billion-android-users-under-the-bus-refuses-to-patch-os-vulnerability.

15 Out-Law.com, "GDPR: Potential Fines for Data Security Breaches More Severe for Data Controllers Than Processors," May 12, 2016, https://www.theregister.co.uk/2016/05/12/gdpr_potential_fines_for_data_security_breaches_more_severe_for_data_controllers_than_processors_says_expert/.

16 Charles Cresson Wood, "Solving the Information Security & Privacy Crisis by Expanding the Scope of Top Management Personal Liability," Journal of Legislation, Vol. 43 (2016), Issue 1, http://scholarship.law.nd.edu/jleg/vol43/iss1/5/.

This dominance is in part brought about by the first group being driven by existing financial, political, and military incentives, while existing political, moral, and humanitarian pressures only drive the second group. This dominance is additionally brought about because the first group, year after year, is realistically projected to be expanding its investment in research and development at a percentage increase far in excess of the percentage increase of the second group.[17]

Think of it as an arms race of sorts. Without significant further investment in rule making and rule enforcement, the second group stands little chance of being able to catch up with the first group, let along bring some semblance of law and order to the increasingly Wild West-like domain of information security and privacy. The implications in terms of eroded information security and privacy in the years ahead are grave because a much greater degree of anarchy and lawlessness is likely without a radically different new legal and regulatory regime, such as the regime that this article suggests be the outcome of a special international convention.

9. Learning via trial and error is now both unduly dangerous and ill-advised

According to traditional English common law, which is still partially subscribed to in the American legal and regulatory system, case law is made via trial and error. Likewise, the traditional approach used by high-tech companies building computer and communications systems was to build it first, get it into the marketplace, and figure out how to add security and privacy later. This learn via trial-and-error approach of high-tech companies has long been supported by governments who didn't want to stifle innovation or impede the high profits of these same high-tech companies. All this is no longer appropriate in an Internet-connected, high-tech world because the trial-and-error approach is now unduly dangerous and expensive.[18]

In a world where hackers can, and have, brought down infrastructure components like reservoir dams and electric grids, the risks are simply too high to keep the old legal regime. The world desperately needs a new legal and regulatory process that brings foresight, insight, and a long-term perspective to information security and privacy matters. That same new approach must be coordinated and cooperative, rapidly learning, and rapidly upgrading. In a tightly-interconnected high-tech world, it no longer works to leave such matters to independent rule-making groups to upgrade laws and regulations when it suits them, to make mistakes as they please and then hopefully learn thereby, or as they please (and in their own time) perhaps learn from the mistakes of others.

Existing models of worldwide rule harmonization that have been successful and some suggested attributes of a successful system-of-rule harmonization, administration, and enforcement

While the authors are not advocating the adoption of any particular organizational model for worldwide harmonization of information security and privacy laws and regulations, there are a significant number of other areas in which such worldwide harmonization of laws and regulations has been shown to be effective, or at least had a reasonable chance of soon becoming effective. These include:

1. ICANN Internet site-naming technical standards
2. ISO toxic material hazard warning labels
3. Maritime laws (law of sea)
4. Antarctica non-development treaty
5. Human rights laws such as the Geneva Conventions
6. UNHCR refugee and displaced person conventions
7. International criminal laws
8. Laws regarding conflict of laws
9. Treaty laws

These examples show that effective, or at least likely-to-soon-be effective, international harmonized legal regimes are a reality. Since there has been some historical experience with these and other harmonized laws, we can be, and should be, learning the lessons that these harmonized laws provide, rather than "reinventing the wheel" the hard way, via trial and error as we go along.

These examples reveal a number of desirable attributes for international harmonized legal systems, which should in turn be applied to the information security and privacy area. These attributes could for instance include:

1. Promotion of cooperation between the authorities in all signatory nations
2. Facilitation of sharing information between signatory nations
3. Protection of shared resources and/or vulnerable populations worldwide
4. Protection of certain nations against the aggressive, confiscatory, or deceptive acts of other nations
5. Leveling of the playing field so that all nations can benefit from a worldwide legal and regulatory regime
6. Provision of an authoritative basis on which international legal proceedings could be based
7. Opportunity to simplify the internal laws and regulations of signatory states

17 Consider that the successful and stable use of a traditional jail/prison to restrict the movements of a prisoner and protect the public requires that there be a large power asymmetry between the jailer and the prisoner, where the jailer holds the clear advantage. But in the case described in this paper, the law breaker (these people are, for the most part, currently not prisoners because the system doesn't work very well) has the clear power advantage. In the latter case, the application of traditional legal and regulatory models, such as the regime now used in information security and privacy, is never going to work.

18 Even large company board members now acknowledge that cyberthreats aren't being adequately dealt with. Consider that in a survey of 5,000 directors, board members ranked cybersecurity preparedness dead last on a list of 23 responsibilities of the board. See J. Yo-Jud Cheng and Boris Groysberg, "Why Boards Aren't Dealing With Cyberthreats," Harvard Business Review, February 22, 2017 – https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats.

8. A new model for international cooperation in the domain of law and regulation development/refinement via a multi-stakeholder participatory process
9. Elimination of needlessly expensive competition between states, freeing-up resources that could instead be used to improve the international legal and regulatory regime

A new information security and privacy regime could thus be distilled from the universe of existing global legal regimes. This new regime could for example include a standard of due care that is uniform across all vendors' equipment and systems, thus explicitly clarifying what must be incorporated into those information systems that are sold, rented, leased, or otherwise provided. This new body of law could also be grounded in principles of avoidance, deterrence, responsibility assignment, and accountability with liability clearly assigned not only to organizations, but also to involved individual decision makers. This new body of law could additionally incorporate incentives that would help to compel information security and privacy decision making such that it would rightly be protecting all those parties that are expected to be materially affected.

Even more potentially useful in the context of information security and privacy rule making are a number of non-traditional organizational structures that, with the aid of information systems technology, have been shown to be exceedingly low-cost, rapidly-evolving, and incredibly accurate. Consider the Dabbawala, a network of lunch box delivery services in India. Through a sophisticated system of box marking and sorting, this network delivers between 175,000 and 200,000 lunch boxes every day, and makes less than one mistake in six million deliveries.[19]

Similar Internet-supported non-hierarchical networks could facilitate a rapidly-evolving new process for information security and privacy rules. While we don't yet know what form this new process should take, we advocate a new international organizational design that dynamically supports super fast law and regulation needs identification, rules formulation, rules adoption, rules implementation, rules enforcement, and rules auditing.

19 Perry Garfinkel, "Delivering Lunch in Mumbai, Across Generations," The New York Times, February 2, 2017, https://www.nytimes.com/2017/02/02/jobs/dabbawalas-india-lunch.html?_r=0.

Suggested next steps

To identify the best organizational form for such a new multi-national rule-making process, we advocate the holding of an international convention where the attendees would:

1. Review existing international law and regulation harmonization efforts to discern what has been working and what has not been working so that the best of those prior efforts can be carried forward into a new proposed regime.
2. Further identify the problems associated with the current information security and privacy rule-making process—a conversation initiated in this article.
3. Define a new and preferable harmonized rule-making process, a process that would be for the benefit of the entire world and not dependent on approval from existing national governments, supra-national entities like the United Nations, major corporations, or major tech firms.
4. Define attributes of this new streamlined process, including an appropriate organizational structure as well as checks and balances, a high degree of transparency and continuous auditing, mechanisms to prevent conflicts of interest, alerts to flag the fact that the process may be compromised, alerts indicating that attempts are being made at compromise, etc.
5. Articulate a way to make decisions via experts who know what the actual risks are, rather than via politicians, corporation top managers, or tech firm vendors.
6. Reconcile the perceived (and largely illusory) loss of jurisdictional sovereignty with the need for a more effective worldwide legal and regulatory regime.
7. Determine how this process will tie-in with the definition of the legal and regulatory standard of due care and a related liability safe harbor.

If you endorse the holding of such a convention, would be interested in attending the convention, or would like to be notified about developments related to the convention and/or reporting on the results of this convention, please sign the petition at http://goo.gl/HS7XXb. This list will be used for only two purposes: (1) showing legislators and other rule-making bodies that there is a significant level of support for the development of a new rule-making process, and (2) contacting

Continued on page 34

could it be that the open source community is too dismissive of liability? I seek to address that question in the following sections by analyzing open source software from the perspective of tort liability rather than the typical contract law that would protect the organizations using these licenses.

Tort liability law

A *tort* is an action that results in some sort of injury—physical, emotional, economical, or otherwise—for which damages may be sought through a civil court case. An individual can make a civil claim against another entity and, with appropriate evidence, circumvent traditional contract law to hold said other entity liable for damages. Torts are largely divided into three different categories: negligence, strict product liability, and intentional interference.

In this article, intentional interference will not be considered. The assumption is made that open source developers have no ill will toward anyone who uses their published software, which is largely true in practice. Instead, analysis will be emphasized with respect to the other two torts: negligence and strict product liability.

Negligence refers to any scenario where an individual or organization, with some duty to one or multiple other entities, acts in a manner that somehow falls short of how a reasonable person would act. In this context, a duty is defined as an obligation, which could be established through a financial transaction, a contract, or some other interaction that would establish a relationship between the two parties. When making a claim of negligence, the plaintiff must be able to prove four facts:

1. Defendant owed a duty to the plaintiff
2. Established duty was breached in some way
3. Injuries incurred by the plaintiff were due to the defendant's breach of duty
4. Injuries incurred by the plaintiff resulted in the damages for which the plaintiff submitted the claim

Strict product liability differs extensively from negligence because it completely disregards the behavior of the manufacturer of the product in question. As its name implies, it is the product that caused the injuries to the plaintiff that is the only point of consideration when evaluating whether or

A Simple Appeal to Common Sense

Continued from page 22

the signers about an upcoming convention and related developments.

Conclusion

When we step back and objectively examine the current legal and regulatory regime for information security and privacy, we note there are many problems, including: (1) jurisdictional fragmentation that creates confusion, unnecessary costs, and lack of meaningful action, (2) an information explosion that overwhelms existing legal decision-making systems, (3) a slow pace of legal rule changes that cannot hope to catch-up with the pace of technological change, (4) a tradition of waiting for crisis to prompt rule changes that now creates undue risks, (5) excessive political and special interest influence that prevents the adoption of suitable new rules, (6) widespread incompatibilities, errors, gaps, and occasionally even contradictions in the law that present attackers with an attractive attack surface, (7) a background of economic incentives that does not cause the marketplace to naturally evolve toward a secure, private, and self-healing state, (8) a situation where attackers invest considerably more resources than protectors, and the gap between those groups is widening, and (9) a reliance of trial-and-error to discover the best legal rules, which is dangerous and ill-advised.

Now is the time for us to let go of our unjustified hope that if only we throw more resources at our antiquated legal and regulatory regime, it's going to work in the area of information security and privacy. The current regime cannot work, and cannot be made to work, and we urgently need a new regime. Just what that new regime should look like is beyond the scope of this article, but those of us working in the field should now have a serious multi-stakeholder conversation about the form this new regime should take.

About the Authors

Charles Cresson Wood, JD, MBA, MSE, CISA, CISM, CISSP, CGEIT, is an attorney, plus independent information security and privacy consultant, based in Mendocino, California. He recently published a law review article in the Journal of Legislation, *entitled "Solving the Information Security and Privacy Crisis." Reach him at ccwood@ix.netcom.com.*

William S. Rogers, Jr., Esq., is chair of Prince Lobel's Data Privacy and Security Practice in Boston, MA. He focuses on compliance, risk management, and breach-related regulatory enforcement and civil litigation. He may be reached at wsrogers@princelobel.com.

Ralph Spencer Poore, PCIP, CFE, CISA, CISSP, CHS-III, X9F1 Vice Chair, has over 45 years of information security experience, including more than 20 years of applied cryptography. He has written extensively on information security and cryptography. Hew may be reached at rspoore@ralph-s-poore.com.