Innovative or Disruptive? – How Cutting-Edge Technologies Could Pose Major IP and Broader Legal Challenges

Masa Noda
Shareholder
Greenberg Traurig, LLP
nodam@gtlaw.com
What is 3D Printing?

> **3D printing** = additive manufacturing process; created layer by layer

> **Traditional design and production process** = subtractive manufacturing, i.e., subtracting material from a larger block
Effects on Manufacturing and Economy

> Complex, detailed shapes can now be created using low-cost, easy-to-use systems operated by individuals, including consumers at home

> Potential to bring production closer to the end user/or the consumer, thereby reducing current supply chain restrictions

> Shipping spare parts may become obsolete → localized production based on demand

> May impact economy both positively and negatively

> Expected to generate $12.8 billion by 2018 and exceed $21 billion by 2020
How Does 3D Printing Work?

> Objects are created by depositing layers of material on top of each other based on a three-dimensional digital map created in software

> 3D printing starts with a blueprint, usually one created with a computer aided design (CAD) program OR a model can be scanned with a 3D scanner

> The model is then “sliced” into layers, converting the design into a file readable by the 3D printer

> The material processed by the 3D printer is then layered according to the design and the process
3D Printers
Benefits and Value of 3D Printing

> Allows for mass customization – ability to personalize products according to individual needs and requirements

> Ability to produce complex products that simply could not be produced physically in any other way

> Eliminate the need for tool productions, i.e., costs, lead times and labor

> Energy-efficient technology
Potential Impact on IP/Brand Owners

Enforcing cases of infringement by 3D printing is and will be extremely difficult

1) Copyright
   - Copying existing commercial product
     ▪ CAD plans can be easily copied and distributed online
     ▪ 3D scanner has capability to create a CAD file by scanning a 3D object

2) Trademark / Trade Dress
   - Products with well-known trademarks or trade dress may be particularly at risk
   - Specificity of 3D printing would allow an individual to replicate an object without replicating the trademark
   - The “Use in Commerce” issue
Potential Impact on IP/Brand Owners

> **Patent**
- Short amount of time of protection but more complete protection
- No exception for independent creation
- No fair use
- No exception for home use (personal use)
- Objects protected by functional patents as well as items protected by design patents, e.g., branded jewelry, can be duplicated without permission

> **Publicity Rights**
- Celebrity’s likeness (if protected by IP) can be replicated, e.g., bobbleheads
Potential Impact on IP/Brand Owners

> Nintendo – Pokemon Bulbasaur Look-Alike Planter Model
Potential Impact on IP/Brand Owners

> Square Enix – 3D-printed Final Fantasy 7 Figures
Potential Impact on IP/Brand Owners
How to Protect IP Assets – Now and in the Future

> **Digital Millennium Copyright Act (DMCA)**
  
  - Provides ISP (Internet Service Providers) immunity from copyright infringement liability
  
  - Removal of 3D printer files online → ISP’s take down allegedly infringing content uploaded to their service by a third party upon receipt of complaint

> **Contributory Patent Infringement**
  
  - Patent owners may go after those who enable individuals to replicate patented items in their homes
  
  - May sue sites that host design files as havens of piracy (can be under copyright law as well)

> **Trade Dress Infringement**
How Businesses Need to Adopt to 3D Printing

> Brand owners should contemplate selling authentic, authorized design files that consumers could print themselves on their 3D printers

> Come up with innovative marketing and distribution models
  - Hasbro, Disney and Wal-Mart have teamed up with a company called 3DPlusMe to allow consumers to have their faces scanned and 3D-printed onto an action figure
3D Printing and the Consumer Goods Industry

Presented by:
Andrew Tsai
Associate General Counsel
Mars, Incorporated
What is 3D Printing?

- It is the creation of a three-dimensional object from a digital model.

- This digital model is made in a CAD (Computer Aided Design) file using a 3-D modeling program (for the creation of a totally new object) or by the 3-D scanning of an existing object. A 3D scanner makes a 3D digital file of an object.

- 3-D printing is also called “additive manufacturing”.

- Objects are created through an additive process – laying down successive layers of material until the entire object is created.
How will 3D printing affect the Consumer Goods industry?

- **Packaging:** It will change how consumers acquire products. Imagine a day when online communities don’t just share opinions about marketing messaging or their experiences, but swap designs for, say, detergent bottles or soap dishes (the premium content will come at a price). It will change the way major consumer brands envision packaging, as products will be stripped of external identifiers and reduced to their very substance. Imagine bags of shampoo on grocery shelves with little more than an identifying tag on them, or bath gel shipped to homes and then ladled into home-printed containers. It will turn many products into constant refills, and have significant impacts on how consumers shop.

- **Products:** Food (including chocolate) can be produced by 3D printing machines

- **Products:** Automotive parts, jewelry, tools, toys, gadgets (e.g. phone cases), eyeglasses etc. can all be produced by 3D printers at a fraction of retail costs
Implications on IP Rights: Patents

- Patents are used to protect a process or product. A patent gives the owner an exclusive right to make, use or sell the invention for a defined period of time in the jurisdiction where the patent is granted.
- Patent infringement can occur by the simple act of printing a 3D copy of a patented object without the permission of the owner.
- No personal use exemption – absence of a commercial purpose is not an exception to patent infringement.
- Example of infringement: even without sale or use
- Hard to police
IP Challenges for the Consumer Goods industry

- Used to protect the “look and feel” of an object such as its shape, pattern, configuration or ornamentation. For example, protection can be obtained for the shape of a food container or the visual features of a running shoe.
Broader Legal Challenges for the Consumer Goods Industry

- Trademark concerns (use My Little Pony licensing example – win for TM holder, 3D printer manufacturer and individual)
- Counterfeit products
- Enhanced product liability concerns
- Copyright of CAD files
- Legislation governing standards
What is the Internet of Things?

• The ability for everyday devices to connect with each other and with people

• Today, there are 6 billion devices connected to the Internet
  ➢ By 2020, estimates put that number as high as 50 billion
  ➢ That’s 4-7 connected devices per person
  ➢ Estimated 6 billion sensors will be shipped in 2015

• At present, most smart products are fragmented and do not work together. Data is siloed in each product’s separate app. That will change in the future as devices grow more inter-connected

• Passive sensors collect and distribute information without the need for a person to activate the sensor each time data are processed

• Leading sectors: healthcare, pharma, energy, automotive
IoT – Definition

• No single definition, but reoccurring key concepts

  • **Oxford Dictionary**: “a proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data”

  • **Wikipedia**: “the network of physical objects or ‘things’ embedded with electronics, software, sensors and connectivity to enable it to achieve greater value and service by exchanging data with the manufacturer, operator and/or other connected devices”

  • **Webopedia.com**: “the ever-growing network of physical objects that feature an IP address for Internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems”

  • **McKinsey**: “sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet”

• So in a nutshell, IoT is about “things,” networks, and services (data analytics)
IoT Timeline - Ancient Times

- 1960's
  - 1969 - Internet is born

- 1980's
  - 1980 - Distributed Sensor Networks (DSN)
  - 1982 - Scout drone (real-time video) placed into service

- 1990's
  - 1990 - first connected "device" (toaster)
  - 1994 - first "smartphone" (BellSouth), first wearable device (WearCam)
  - 1995 - first GPS navigation system (GM GuideStar)
  - 1999 - the phrase "Internet of Things" is coined
IoT Timeline - Recent History

• 2000
  • first internet-connected refrigerator (LG)
  • precise GPS made available to consumer market (Pres. Clinton)
• 2001 - first 3G network (NTT DoCoMo)
• 2002 - Ambient Orb
• 2008 - birth of the IoT
• 2011 - Nest thermostat
• 2012 - Google Glass
• 2014 - Apple HomeKit & HealthKit; Google driverless car (prototype)
What is a “thing”?  

• The term IoT was first coined by the Auto-ID center in 1999, as part of efforts under way with respect to standardizing approaches to RFID tags.

• One way to think about “things” are by their communication patterns (IETF Security Considerations Draft (2013)):
  
  ➢ human-to-human (H2H)
  ➢ human-to-thing (H2T)
  ➢ thing-to-thing (T2T)
  ➢ thing-to-things (T2Ts)

• Sensors, microcontrollers, sensor hubs, mobile devices and more hubs take in and compute data remotely, in the cloud, to relieve processing required on the sensor’s application processor or the microcontroller.

• IPv6 and web services simplifies deployment by enabling simplified integration with Internet hosts, simplified development of diverse “things” and a unified interface for software.
Internet of “Things”

• **Internet of SELF:**
  • Wearable devices (FitBit, Microsoft Band, Nike FuelBand, Jawbone Up)

• **Internet of CAR:**
  • Infotainment and telematics systems (BMW Connected Drive, GM OnStar)

• **Internet of HOME:**
  • Security monitoring, automatic/remote access and control (Nest, Control4 Home Automation, Comcast Xfinity Home, Jibo, Amazon Dash)

• **Internet of INDUSTRY:**
  • Asset and performance monitoring, predictive maintenance (GE – Industrial Internet, Cisco – Internet of Everything, IBM – Smarter Planet)

• **And so much more:** Health, Schools, Agriculture, Cities, etc.
2015: A Day in the Life...

- Eating breakfast: smart fridge
- Getting dressed: wearable tech
- In the car: connected apps
- The connected workplace
- Shopping and errands:
- Personalized retail
- Smart home: from smart thermostats to smart sensors
- Entertainment
IoT - Network

• **Bandwidth**
  - Capacity to facilitate connections between ever-increasing number of IoT devices and backend data repositories

• **Connectivity**
  - Ability to reliably connect devices anytime, anywhere
IoT – Hardware/Software Backend

• Backend could be on-premises or in-cloud
• But cloud infrastructure is tailor-made for IoT – available on-demand and optimized for:
  • Telemetry
  • Big Data
  • Analytics
  • Machine Learning
Key Functions required by IoT

• **Device and Infrastructure Management Platform**
  - Automated provisioning of edge devices to ease deployment
  - IoT requires operators to operate software on devices remotely, without taking the network of sensors out of service

• **New Platform-as-a-Service (PAAS) offerings emerging for Big Data**
  - Data storage (e.g., supported versions of Hadoop); data warehousing and database tools
  - Data normalization techniques to improve interoperability
  - Data analytics tools and applications: real-time and predictive

• **Data Filtering**
  - Vast amounts of data can be generated by sensors
  - Need to filter data to that which is necessary so that systems aren’t overwhelmed

• **Analytics Platform**
  - Diversity of devices producing data from different locations need to be configured so that the data can be leveraged
  - Integration with the big data analytics platforms

• **Security by Design**
So are there any legal issues?

- Wide range of issues including:
  - Privacy
  - Data Ownership/Rights
  - Security
  - Liability Risks
  - IP Rights/Licensing
Privacy

• Which law applies?

• What individuals and what data are covered?

• When data are collected and by whom?

• Organizations must demonstrate legitimate interest or obtain consent

• Risk of data use for incompatible purposes

• Data security – multilayered and expensive to implement
Data Ownership/Rights

• Who has access to my data?
  • What is disclosed to customer? And how?
  • How might these disclosures vary between consumer and enterprise IoT?
  • What rights does law enforcement have to access this data?

• For what purposes?
  • Again, what are the disclosures?
  • Service improvement only? Advertising? Other secondary uses?
  • How might IoT generate new commercial opportunities for the customer whose “things” are generating data?

• What are you doing to protect my data from unauthorized access/use?
  • What cloud security technologies are available?
  • Are there any disclosure requirements?
  • What about regulatory requirements or voluntary security frameworks?
Security

• **The Concern**: Unauthorized access and control of devices can result in a variety of types of harm

• **Threats to the Individual**
  • Threats to physical safety (remote programming of pacemaker, drug dispensers or smart meter)
  • The changing face of identity theft: i.e. “identity” extends to our objects, to the “things” that track our behavior and can then be used to threaten us personally
  • Ransomware: the ability to threaten someone with knowledge of sensitive information (e.g., unauthorized access to data from pill sensor)
  • Traceability and unlawful profiling

• **Threats to corporations and other entities**
  • Corporate theft and espionage e.g. IP theft
  • Tangible property
  • Physical security
  • Data security

• **Cyberwar and cyber-terrorism**
  • Public safety, threats to critical infrastructure
Liability Risks

• Managing Risk
  ➢ IP reps
  ➢ Legal Compliance programs: consent to use data, privacy policies, data breach notification, etc.
  ➢ Security Procedures
  ➢ Contractual Indemnity: tied to above
  ➢ Insurance

• Traditional allocations of liability may need to be re-examined
  ➢ How do traditional concepts of direct and indirect loss cope?
  ➢ Application of norms of legal foreseeability

• Address liability holistically across entire range of contractual arrangements

• Consider supply chain indemnities

• Evaluate liability caps for emerging types of harm
IP Rights/Licensing

• Who owns the IPR in the data collected?

• IPRs
  • Copyright, Database Rights, Moral Rights, Trademarks, Trade Secrets/Confidential Information

• Data Sources
  • Proprietary, Open, Creative Commons, Public Domain

• Big data involves analytics which requires copying and processing the data

• Key question: are your ownership & license rights wide enough to cover the intended use?
Patent Issues: Divided Infringement

Divided Infringement: does anyone directly infringe the claims?


- one who "acts through an agent (applying traditional agency principles) or contracts with another to perform one or more steps of a claimed method"
- one who "conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance"
- "where two or more actors form a joint enterprise, all can be charged with the acts of the other, rendering each liable for the steps performed by the other as if each is a single actor"
Patent Issues: Valuation/Damages

Apportionment: what is the value of the claimed invention?

• Generally, assess the value of the component/feature embodying the claims.

• May only use the value of the entire product when:
  • the patented feature creates the basis for the customers’ demand for the product, or the patented feature substantially creates the value of the other component parts of the product; or
  • the product in question constitutes the smallest saleable unit containing the patented feature.

• VirnetX, Inc. v. Cisco Systems, Inc., 767 F.3d 1308 (Fed. Cir. Sep. 16, 2014) (reversing the district court's decision to allow plaintiff to use the value of an iPhone to assess damages for patents asserted against two software features) ("Where the smallest salable unit is, in fact, a multi-component product containing several non-infringing features with no relation to the patented feature . . . , the patentee must do more to estimate what portion of the value of that product is attributable to the patented technology")
Conclusions & Takeaways

• IoT and Big Data present significant legal challenges
  ➢ Compliance with Law, Global Commerce and Managing within a Changing Legal Landscape
  ➢ Privacy
  ➢ IPR and Data Ownership

• Understand the data – and track issues accordingly
• Focus on Privacy-by-Design and Security-by-Design
• Consider approach to allocation of liability
• Understand the supply chain and address its issues
• Track the legal and regulatory developments
Contact Info

• Hogene L. Choi
  • Senior Associate, Baker Botts
  • hogene.choi@bakerbotts.com

• Vineet Shahani
  • Head of Product and Commercial Legal, Nest Labs, Inc.
  • vineet@nestlabs.com

• Jae B. Pak
  • Senior Attorney, Microsoft Corporation
  • jae.pak@microsoft.com
Disruptive Technology


Disruption: In the past two decades, the concept has gone from theory, to buzz word, to the captivation of the popular imagination. Disruptive innovation goes beyond improving existing products; it seeks to tap unforeseen markets, create products to solve problems consumers don’t know that they have, and ultimately to change the face of industry. We are all the beneficiaries of disruption. Every smartphone carrying, MP3-listening, Netflix-watching consumer is taking advantage of technologies once unimaginable, but that now feel indispensable. Silicon Valley’s pursuit of disruption will continue to benefit and delight a world of consumers. But where disruption may once have been the secondary result of innovation, disruption has become a goal in and of itself. Today, I want to urge a cautionary note: The tech community’s solipsistic focus on disruption, to the exclusion of human and legal values, can be problematic. We can see these potential problems in the development of three areas: mass surveillance, 3D printing, and driverless cars. SEE ATTACHED PDF.

- **Wearable cameras** is making it easier than ever to constantly, discreetly photograph and record those around you and instantly upload the images and video to the internet.
  - However, wearable cameras and computers present several concerns: they may infringe on privacy; and they can violate social norms. People are often annoyed and downright angered by the possibility of being filmed in public without their consent—leading sometimes to episodes of violence against users. These concerns are exacerbated by the potential for facial recognition software.
  - Wearable cameras threaten individual privacy.

- Since its birth in the 1980s, **3D printing** has morphed from an area of research to the mainstream. We have 3D printed drones, prosthetic limbs, and blood vessels. 3D printing is becoming accessible, with printer models available for under $500.
  - 3D printing could help startups by increasing the ease of experimentation. New companies could design, print, and test new creations quickly and cost-effectively in-house.
  - The potential to print dangerous things, such as unregulated and undetectable plastic guns, exists. Drugs—both prescription and illicit—could be printed at home, without the safety net of FDA inspection or approval. Home-printed objects in general, such as children’s toys, would not have the benefit of testing and inspection. 3D printing could also create major economic dislocation. Millions of people in factories could lose their jobs.
  - How should we think about the **patentability** of 3D printed organs made from human cells? 3D printing also presents a generalized challenge to intellectual property. 3D printing removes the traditional barriers to production, making patent, copyright, and trademark infringement easy. It has the potential to cripple the intellectual property system and chill innovation. Inventors may be wary of pouring time and finances into something that people will copy and print for themselves instead of purchasing.
• **Self-driving cars** will be available to the public within this decade, and the legal roads are being paved now in anticipation. Nevada, Florida, California, and D.C. have passed laws permitting the testing and use of autonomous cars, and further legislation is pending in many other states.
  o Could reduce car accidents due to human error, and could reduce traffic congestion and fuel consumption.
  o Autonomous vehicles could potentially threaten jobs: in the freight and transportation industries, buses and tractor trailers could begin to drive themselves, and traffic cops would no longer be necessary. Self-driving vehicles would also open the country up to a number of new security concerns. Hackers could tamper with autonomous driving software; terrorists could infiltrate the central transportation system.
  o Liability in a world of driverless cars is one of the great legal questions to come. Accidents will happen, and the questions of responsibility and cost will be complicated. We currently have no legal framework for such liability.


...the two common threads running through discussions about the legal risks they pose are data security and consumer privacy. This article addresses legal issues and risk in these technology areas: **Bring Your Own Device (BYOD)**, big data, the Internet of Things (IoT), cloud/Software as a Service (SaaS), and social media.

• **BYOD** is no longer a trend. Many employees fully expect it, and it’s increasingly difficult for companies to just say no.
  o The single greatest risk with BYOD is the potential loss of enterprise data. With personal devices, there is no way for a company to ensure that only their staff members will have access to them. If an employee in the healthcare industry, for example, loses a device containing patient data, the risks of litigation and regulatory response could be substantial.
  o Wiping a mobile device: A common protection for BYOD data loss is for a company to completely wipe the data from a lost mobile device; companies should obtain consent from employees to take this measure. But what if a firm wipes mobile data by mistake? And what happens if an employee had media downloads on the device to the tune of hundreds of dollars? If an employee refuses to sign a waiver permitting data wiping, what can a company do? Legal ambiguities and pitfalls abound in this kind of approach. And have you adequately warned staff that their personal devices — and possibly all the personal information that’s on them — could be subject to legal discovery?

• **Major takeaways of BYOD: you need an effective BYOD policy, and the right tech solution is critical.**

• Need to examine the risks to **data security and individual privacy involving Big Data.**
  o Large data sets: In big data the amounts of information are very large and come from multiple sources. Despite the efforts of collectors and analyst firms to de-identify data
from smartphones, geo-location platforms, and other sensitive sources, without adequate protections hackers can potentially re-identify individuals; this could result in litigation and is a very real risk (the amounts and concentrations of data are tempting for criminal interests). It has been argued that big data could open up more automated forms of discrimination when private sector firms (e.g., health insurance providers) make complicated decisions about consumers. This is an area where consumer advocacy and legislation have to play a role.

- **Legal discovery:** With large datasets and the types of raw, unprocessed data involved, a firm's efforts to limit the scope of legal discovery could prove difficult; this could open up sensitive and proprietary information to outsiders' scrutiny. Regarding the use and publication of big data analyses, an enterprise has to evaluate the potential legal risks. And with an eye to the pitfalls of storing diverse kinds of consumer data, IT leaders need to ask exactly what kinds of information their company should collect and retain.

- **Major takeaways regarding data:** Companies need a set of best practices and effective solutions and must review procedures and contracts of 3rd-party vendors against data breaches. Best practices include auditing access to data, monitoring and logging of actions, and clarifying the chain of data custody. Enterprise-wide efforts have the potential benefit of making risk management an integral part of corporate culture.

- **Anticipate and investigate the profound changes and legal risks that IoT will create.**
  - Predictions about the number of "cyber-physical devices" by the year 2020 range from 20 billion to 50 billion.
  - Data ownership and product liability: Once IoT devices are purchased and enabled, who will own the data they collect? A key legal protection for companies will be not misrepresenting their products.
  - Customer privacy concerns: How will consumers be given reasonable notices about privacy and be able to indicate their preferences when the devices have no user interfaces? Businesses should respect consumer privacy and seek to make data anonymous, as well as be open and transparent about their uses of data.
  - Network security may not be a primary competence for many IoT device makers, and that will have to change. Due to the nature and volume of the data collected, it is not a matter of when or if criminal interests will target IoT networks. Both the government and relevant industry sectors will have to be proactive in this regard.

- **A careful review of the legal risks for cloud providers and customers is necessary.**
  - Data security: One of the main differences between traditional software and a cloud/SaaS agreement is where customer data is located. In a SaaS transaction, a customer is storing some of its potentially sensitive data with the cloud provider.
  - Service level agreements (SLAs): SLAs, the written commitments a service provider makes regarding levels of service, support, and downtime penalties, have become a standard element of the cloud business model. Crafting the right agreement for a cloud-
based firm demands technological know-how and experience in drafting and negotiating SaaS business contracts.

- Data encryption and legal discovery: Most standard cloud contracts state that the provider will comply with all subpoenas for data, which means a cloud provider will straightaway provide company data to the entity issuing the subpoena — potentially without the customer's knowledge. Encryption of data stored with a cloud provider can give an added layer of protection in such cases. Even if a firm has to comply, at least it will need to provide the encryption key for the data, and thus be alerted to an unfolding legal process.

- **Social media** and the unpredictable nature of user-generated content and the ongoing legal risks are worth highlighting.
  - Privacy and posting sensitive information: The Federal Trade Commission has issued its privacy guidelines regarding the protection of online personal data, which businesses and legal advisors need to be apprised of. For employees, there is inherent risk in placing personal information online about schedules and activities; these can enable tracking. There is also the risk of inadvertently sharing sensitive or confidential information through social media. Clear, written guidelines about appropriate posting and sharing are necessary.
  - Employment screening: Businesses need to refrain from using a site such as Facebook during the hiring process. If litigation uncovers that an employer learned about sensitive personal information (such as age, family status, political profile, or sexual orientation) via social networks, and then turned down a candidate on the basis of information it would not otherwise be privy to, it can be held liable.
  - **Intellectual property**: Along with vigilant online reputation management, a business has to monitor its brand online to protect its registered trademarks. Not challenging third-party uses of a registered trademark could result in its loss via abandonment. Think of brands such as Kleenex, Xerox, Thermos, and Coca-Cola and the legal efforts they have undertaken to protect their brand names. The US government does not monitor third-party usage, so it is up to the trademark holder to do so.

- **Major takeaway regarding social media**: Have a social media policy. Write a clear, effective, and enforceable privacy and social media policy. Train your staff on its provisions and implications, and above all be consistent when enforcing it.
INTRODUCTION

Disruptive Technologies and the Law

Neal Katyal*

It’s great to be here with all of you. This symposium actually has its origins in a sort of technology: I was on a flight to Silicon Valley, and despite living thousands of miles away from him, bumped into Professor Desai. We got to talking about disruptive technology, and ultimately began spinning out thoughts on 3D printing. Soon thereafter The Georgetown Law Journal asked for ideas for their symposium, and thus this fantastic event was born.

Disruption: In the past two decades, the concept has gone from theory, to buzz word, to the captivation of the popular imagination. Disruptive innovation goes beyond improving existing products; it seeks to tap unforeseen markets, create products to solve problems consumers don’t know that they have, and ultimately to change the face of industry. We are all the beneficiaries of disruption. Every smartphone carrying, MP3-listening, Netflix-watching consumer is taking advantage of technologies once unimaginable, but that now feel indispensable. Silicon Valley’s pursuit of disruption will continue to benefit and delight a world of consumers. But where disruption may once have been the secondary result of innovation, disruption has become a goal in and of itself. Today, I want to urge a cautionary note: The tech community’s solipsistic focus on disruption, to the exclusion of human and legal values, can be problematic. We can see these potential problems in the development of three areas: mass surveillance, 3D printing, and driverless cars.

In 1890, in their classic article establishing a right to privacy, Louis Brandeis and Samuel Warren wrote, technologies “have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”¹ This passage appears quaint today in its details; it refers to the new Kodak “[i]nstantaneous photographs” and the “unauthorized circulation of portraits of private persons.”² But the sentiment, and the argument in favor of a legal right to privacy, applies equally today.

After all, cameras were once bulky, noisy devices, and unwilling subjects at least knew that they were being photographed. Today, virtually everyone has a noiseless, unobtrusive camera in the form of a smartphone. And the prolifera-

* Paul and Patricia Saunders Professor of Law, Georgetown University. © 2014, Neal Katyal. This piece is a transcription of Professor Katyal’s oral remarks that introduced the Symposium on November 8, 2013. He wishes to thank McKaye Neumeister, Yale Law School class of 2017, for terrific research assistance.

2. Id.
tion of wearable cameras is making it easier than ever to constantly, discreetly photograph and record those around you and instantly upload the images and video to the internet. Consider Eye-Tap, an over-eye camera developed by Dr. Steve Mann, who has been developing and using wearable cameras and computers since the late 1970s. Consider smart watches with recording capabilities. And consider innovations like Google Glass that incorporate “heads-up displays,” so that users do not have to look away from their lines of sight.

Wearable computers and their cameras present great benefits. They’re hands free, less bulky and distracting than traditional cameras, and they allow users to seamlessly record their life as it happens. I can take a picture of my kids, for example, without a hitch. Some police departments are also using wearable cameras, having officers attach them to a hat, collar, or sunglasses. However, wearable cameras and computers present several concerns. For starters: a) they can look ridiculous; b) they may infringe on privacy; and c) they can violate social norms. People are often annoyed and downright angered by the possibility of being filmed in public without their consent—leading sometimes to episodes of violence against users. These concerns are exacerbated by the potential for facial recognition software. Google has said it will not make these features available on Glass “without having strong privacy protections in place.” However, hackers will find ways around this prohibition. The potential for constant public identification and surveillance is unnerving generally. And in certain situations it completely flaunts social norms. Some bars, casinos, and strip clubs have already instituted bans on the technology.

Wearable cameras are just one aspect of disruptive technology that threatens individual privacy. As Professor Slobogin has discussed in his paper for this symposium, there is a risk of “panvasive surveillance” through fusion centers, domestic drones, cameras, and the collection of communications metadata. These techniques can undoubtedly have positive effects. Cameras can locate missing persons, alert authorities to suspicious packages, and solve crimes. In fact, such cameras were used to help identify and find the Boston Marathon bombers and the London Underground bombers.

But the ease and broad scope of this surveillance raises serious social and legal questions about the right to privacy. Recall, for instance, United States v. Jones, in which the Supreme Court held that the Government’s attachment of a GPS device to the suspect’s vehicle constituted a search under the Fourth Amendment. Many in law enforcement had thought that these forms of tracking were not problematic: if the Government could pay a police officer to monitor a vehicle 24 hours a day, why should the result be different if technology does the work instead? But the Government missed the key lesson of

cyberspace—something Larry Lessig realized many years ago in his first cyber-

space book, *Code*—that a difference in degree can become a difference in kind

with enough technology. Today, I worry that Silicon Valley gets too enamored

by tech and has not fully internalized Lessig’s lesson. A difference in degree can

sometimes morph into a difference in kind, making extrapolation from our past
to the new advanced technological age a fraught endeavor.

A second up-and-coming technology to consider is 3D printing. Since its

birth in the 1980s, 3D printing has morphed from an area of research to the

mainstream. We have 3D printed drones, prosthetic limbs, and blood vessels.
3D printing is becoming accessible, with printer models available for under

$500.

As Professors Desai and Magliocca note in their paper for this symposium,
3D printing could help startups by increasing the ease of experimentation. New
companies could design, print, and test new creations quickly and cost-
effectively in-house. New ideas will carry less financial risk. As GE has found,
3D printing can also help bigger companies produce components. This could
ultimately bring manufacturing back to America from overseas. 3D printing
may even decrease pollution, as it reduces the need for shipping. And individu-
als will have access to goods that they couldn’t find in the store or wouldn’t
otherwise be able to afford.

Beyond the realm of manufacturing, the possibilities are endless. 3D printing
could revolutionize medicine. The technology is already being used to produce
prosthetic hands. Doctors are experimenting with custom 3D printed casts
to support broken bones. Others are working to print the bones themselves.
And 3D firms are working on printing 3D organs with a patient’s own cells.
Someday, 3D printing could provide an organ to each of the thousands of people
on the national organ donor waiting list.

The disruptive effects of 3D printing are sure to be felt in a number of
industries, in ways we cannot yet imagine. But some problems are easy to
predict. The one that has captured the public’s imagination is the potential to
print dangerous things, such as unregulated and undetectable plastic guns. This
past May an engineer uploaded a video to the internet in which he tested a 3D
printed gun, made with only $25 of plastic. However, as Professors Desai and
Magliocca note, the gun issue may very well be a red herring, and there may be
several ways to regulate the 3D printing of firearms. Apart from weapons, 3D
printing carries the potential for individuals to get hold of other unsafe products.
Drugs—both prescription and illicit—could be printed at home, without the
safety net of FDA inspection or approval. And home-printed objects in general,
such as children’s toys, would not have the benefit of testing and inspection.

Beyond the nefarious, 3D printing could create major economic dislocation.
Millions of people in factories could lose their jobs. And apart from that, the
technology poses new and interesting legal questions. For example, how should

we think about the patentability of 3D printed organs made from human cells? 3D printing also presents a generalized challenge to intellectual property. 3D printing removes the traditional barriers to production, making patent, copyright, and trademark infringement easy. It has the potential to cripple the intellectual property system and chill innovation. Inventors may be wary of pouring time and finances into something that people will copy and print for themselves instead of purchasing.

The law must adapt to this future. Professors Desai and Magliocca begin the process of thinking through the potential threats to intellectual property and how the law can evolve to accommodate this exciting area of innovation. How should the law treat the threat that 3D printing poses to workers’ livelihoods? Issues of safety and regulation? The potential moral and ethical questions raised by bio-printing? These debates will play a role in the evolution of the law.

Finally, a third technology discussed in this symposium is driverless cars. Self-driving cars will be available to the public within this decade, and the legal roads are being paved now in anticipation. Nevada, Florida, California, and D.C. have passed laws permitting the testing and use of autonomous cars, and further legislation is pending in many other states.

Of the numerous potential benefits of self-driving cars, the foremost is safety. There are 5.5 million total car crashes in the U.S. per year.\(^7\) Driver error is the primary factor in 93% of crashes.\(^8\) Over 30,000 crashes per year are fatal.\(^9\) Of fatal crashes, over 40% involve alcohol, distraction, drugs, and/or fatigue.\(^10\) The economic cost of crashes in the U.S. is $300 billion per year, or 2% of GDP.\(^11\) Traffic crashes are the primary cause of death of Americans ages fifteen to twenty-four.\(^12\) With the implementation of driverless cars, researchers predict fatality rates could ultimately fall to 1% of current rates.\(^13\) Even if autonomous vehicles constituted only 10% of total cars on the road, it would save 1,100 lives per year.\(^14\) With 90% penetration, the U.S. would save 21,700 lives and have 4.2 million fewer crashes. Per year.\(^15\)

Consider also the reduction in congestion and fuel consumption. Twenty-five percent of congestion is caused by traffic incidents—which autonomous vehicles would largely avoid.\(^16\) They would communicate with one another and the overall transportation system, monitoring traffic patterns and choosing the

\(^8\) Id.
\(^9\) Id. at 3.
\(^10\) Id.
\(^11\) Id. at 4 tbl.1.
\(^12\) Id. at 3.
\(^13\) Id. at 4.
\(^14\) Id. at 8 tbl.2.
\(^15\) Id.
\(^16\) Id. at 5.
best route. And they would travel closer together (more like a train than a
conventional car) and at higher potential speeds, increasing highway capacity
and minimizing traffic congestion. At 90% penetration, American drivers would
save a total of 2772 million hours of travel time, and 724 million gallons of fuel
per year.17 Including the potential reduction of crashes, traffic, and fuel con-
sumption, it is estimated that self-driving cars could save the U.S. economy
$450 billion annually.18

Statistics aside, self-driving cars will provide important social benefits.
They could provide transportation for the disabled and elderly who are currently
unable to drive themselves, giving them increased mobility and independence.
They could transport children without a human driver, easing the burden on
overworked parents. People would no longer need to focus on the road while
behind the wheel. Instead, they could be productive, able to do work or focus on
their families. Self-driving cars would also make parking significantly easier.
Large parking lots and parking scarcity would be things of the past (in much the
same way as the phenomenon of being “lost” is today).

But there are also downsides to this new technology. Autonomous vehicles
could potentially threaten jobs: in the freight and transportation industries, buses
and tractor trailers could begin to drive themselves, and traffic cops would no
longer be necessary. Self-driving vehicles would also open the country up to a
number of new security concerns. Hackers could tamper with autonomous
driving software; terrorists could infiltrate the central transportation system.

Liability in a world of driverless cars is one of the great legal questions
to come. Accidents will happen, and the questions of responsibility and cost
will be complicated. We currently have no legal framework for such liability.
Professor Smith’s discussion of changing liability in light of certain disruptive
technologies is the starting point for considering the changing relationship
between seller and consumer, and tort liability in a future of driverless cars.

All of the technologies discussed in this symposium are truly disruptive, in
the best sense. They will become inseparable parts of modern life because they
serve important social needs. Wearable cameras and computers allow us to
share our lives and participate in the digital community. 3D printing quenches
our thirst for innovation and self-sufficient production. And driverless cars will
save us time, fuel, and lives while increasing mobility and allowing us to focus
on what really matters. But we cannot forget the potential harms, such as the
invasion of privacy, violation of intellectual property rights, and liability con-
cerns surrounding this technology. The law must fill this gap. That is, after all,
what the law is about: Providing human values in an age where technology
causes both profound wonderment and profound disruption.

17. *Id.* at 8 tbl.2.
18. *Id.* at 17.